(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11883 A1

(51) International Patent Classification⁷: H04N 7/167

(21) International Application Number: PCT/US00/21337

(22) International Filing Date: 2 August 2000 (02.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/371,755 10 August 1999 (10.08.1999) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **PATEL, Baiju, V.** [US/US]; 10552 NW La Cassal Crest Lane, Portland, OR 97229 (US). **BAUGHER, Mark, J.** [US/US]; 8608 SW 64th Avenue, Portland, OR 97129 (US).

(74) Agents: **MALLIE, Michael, J.** et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

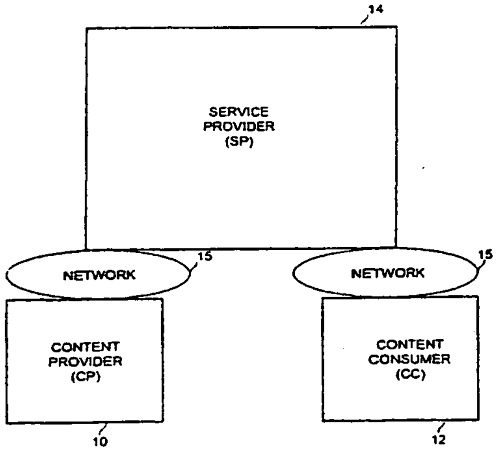
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURELY DISTRIBUTING CONTENT TO GROUPS OF RECEIVERS



WO 01/11883 A1

(57) **Abstract:** An inter-network conditional access system unifies network security and application/content security in a single system to protect a service provider's service and to secure a content provider's content in a multicast network environment. The system includes at least one content provider to provide digital content, and at least one service provider to securely receive the digital content from the at least one content provider and to securely distribute the digital content. The content provider and the service provider may create a relationship of trust between themselves. The system also includes at least one content consumer to securely receive the digital content from the at least one service provider and to securely consume the digital content. The content consumer and the service provider also may create a relationship of trust between themselves.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR SECURELY DISTRIBUTING CONTENT TO GROUPS OF RECEIVERS

BACKGROUND

1. FIELD

The present invention relates generally to data communications and, more specifically, to protection of digital content distributed over a multicast network.

2. DESCRIPTION

Conditional access controls are sometimes used by television (TV) networks where content (e.g., subscriptions to packages of channels) is sold to customers. Conditional access controls permit individual, authorized receivers to receive selected content on a broadcast network, while denying access to the content to unauthorized receivers. TV networks may be analog or digital and there are at least several conditional access control mechanisms available for each type of service. Conditional access controls provide at least two common functions. First, conditional access controls protect the operator of a broadcast network from theft of content by non-paying or other unauthorized customers. This function is important for home TV systems. Second, many conditional access controls use encryption to prevent theft of service. Conditional access controls have been promoted as a security solution for customers of business TV networks who are sensitive to having their business content disseminated unprotected over broadcast networks (such as satellite networks, for example).

Since digital TV content may also include data content, which may have a much higher value than traditional analog content (because original content can be retransmitted without any loss of information), and the same digital content may be distributed to selected groups of customers using multicast or unicast protocols for either data streams or files, additional functions for conditional access controls are desired to ensure that distributed digital content is protected against theft at the destinations to deter unauthorized copying and reuse of high-value data content.

Securing content that is multicast to a large group of customers may be accomplished through the use of symmetric key cryptography, asymmetric key cryptography, or both (e.g., a hybrid approach). One approach is to use public key cryptography for authentication of the receiver prior to multicast distribution of the data, and to use a symmetric key to encrypt the multicast content. Once the receiver is authenticated, the receiver is given the symmetric key to decrypt the content.

One security limitation with this approach is that if one of the authorized receivers decides to share the symmetric key with unauthorized receivers, the unauthorized receivers may be able to receive the multicast content. The risks associated with this problem increase when there are a very large number of authorized receivers, because there are more receivers who can violate the trust of the arrangement and distribute the key to unauthorized receivers. For example, when the multicast content is distributed by satellite, if one of the authorized receivers decides to redistribute the key used for decryption, access to the content may become unlimited. Thus, if the receiver is authorized to receive the content, but is not trusted with the keys to that content, the keys may be protected through various known tamper resistant methods embedded in a trusted viewer application. This scheme complements communications security by protecting the keys used for communications security.

Hence, a mechanism combining communication security with content protection in a system is desired to protect multicast content both during transmission and upon reception within a broadcast or multicast network.

SUMMARY

An embodiment of the present invention comprises an inter-network conditional access system for digital content. The system includes at least one content provider to provide digital content, and at least one service provider, communicatively coupled to at least one content provider, to securely receive the digital content from at least one content provider and to securely distribute the digital content. The content provider and the service provider may create a relationship of trust between themselves in one embodiment.

Another embodiment of the present invention comprises a method of providing digital content in an inter-network conditional access system. The method includes encrypting digital content with at least one key, transmitting the encrypted digital content to at least one service provider, requesting creation of a secure channel for distribution of the encrypted digital content by at least one service provider, requesting creation of a program of data to be sent on the channel, the program comprising the encrypted digital content, and installing the at least one key at a content consumer for decrypting the program.

Another embodiment of the present invention comprises a method of providing digital content service in an inter-network conditional access system. The method includes receiving encrypted digital content from at least one content provider, creating a secure channel for distribution of the encrypted digital content (a program), creating security keys for the program and sending the keys on the channel. In this embodiment, a key protects multiple digital content in the form of multiple programs of data to be distributed to a subscriber base using a cryptographic key for those programs.

Another embodiment of the present invention comprises a method of consuming content in an inter-network conditional access system. The method includes receiving keys that were distributed on a secure channel, receiving a first key for gaining access to the secure channel, receiving a second key for decrypting the program communicated over the secure channel, the program comprising encrypted digital content, decrypting the program key on the channel using the first key, and decrypting the encrypted digital content using the second key.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a diagram illustrating three subsystems of an inter-network conditional access (ICA) system according to an embodiment of the present invention;

Figure 2 is a diagram showing interfaces between a content provider (CP), a service provider (SP), and a content consumer (CC) according to the ICA system of Figure 1;

Figure 3 is a diagram illustrating operations of a new channel function according to an embodiment of the present invention;

Figure 4 is a diagram illustrating operations of an add service provider channel member function according to an embodiment of the present invention;

Figure 5 is a diagram illustrating operations of an add content provider channel member function according to an embodiment of the present invention;

Figure 6 is a diagram illustrating operations of a remove service provider channel member function according to an embodiment of the present invention;

Figure 7 is a diagram illustrating operations of a remove content provider channel member function according to an embodiment of the present invention;

Figure 8 is a diagram illustrating operations of a new program function according to an embodiment of the present invention;

Figure 9 is a flow diagram illustrating an authentication/authorization operation according to an embodiment of the present invention;

Figure 10 is a flow diagram illustrating a content provider request channel operation according to an embodiment of the present invention;

Figure 11 is a flow diagram illustrating a service provider request channel operation according to an embodiment of the present invention;

Figure 12 is a flow diagram illustrating content provider and service provider assign channel keys operations according to an embodiment of the present invention;

Figure 13 is a flow diagram illustrating a content consumer assign channel keys operation according to an embodiment of the present invention;

Figure 14 is a flow diagram illustrating a service provider or content provider assign program keys operation according to an embodiment of the present invention;

Figure 15 is a flow diagram illustrating a content consumer key program operation according to an embodiment of the present invention; and

Figure 16 is a diagram illustrating a sample system suitable to be programmed according to an embodiment of methods of performing content provider, service provider and/or content consumer operations in accordance with the present invention.

DETAILED DESCRIPTION

In the following description, for purposes of explanation, specific numbers, materials, and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well-known features are omitted or simplified in order not to obscure the present invention. Furthermore, for ease of understanding, certain method steps are delineated as separate blocks, however, those skilled in the art will appreciate that such separately delineated blocks should not be construed as necessarily conferring an order dependency in their performance. Reference in the specification to "one embodiment" or "an embodiment" of the present invention means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearances of the phrase "in one embodiment" appearing in various places throughout the specification are not necessarily all referring to the same embodiment.

I. System Overview and Definitions

An embodiment of the present invention includes a system and method for combining network security and application/content security to protect a service provider's data service and a content provider's data content in a multicast network environment. An embodiment of the present invention allows security to be controlled and implemented from different locations within a network, such as at the content provider's location, at the service provider's network operations center (NOC), and at intermediate caching server systems.

In embodiments of the present invention, conditional access may be applied to network environments supporting digital content distribution to receivers such as general purpose computer systems (e.g., personal computers (PC), and servers), although other devices such as set-top boxes, Internet appliances, digital televisions, televisions offering data services, and other data receiving devices, may also be used as content receivers. Generally, digital content may be any digital data. In one embodiment using data formatted according to the Moving Picture Experts Group (MPEG) 2 standard (International Standards Organization (ISO) IS-13818), digital content comprises Internet Protocol (IP) packets that are in the data services layer of an MPEG-2 transport stream. Figure 1 is a diagram illustrating three subsystems of an inter-network conditional access (ICA) system according to an embodiment of the present invention. A content provider (CP) 10 functions as a source of content. The CP may be a general purpose computer system programmed for authoring or other generation and distribution of multimedia data content. Alternatively, the CP may be any source of multimedia data, including a source of live data, such as may be received from motion picture cameras, video cameras, still cameras, and microphones, for example. A content consumer (CC) 12 functions as a consumer or user of the content provided by the CP. The CC may be a general purpose computer system (e.g., a PC or a server), set-top box, Internet appliance, consumer electronics product, digital television, a television (TV) offering data services, or other content receiving device. The CP and CC may be coupled to communications networks 15 such as a public switched telephone network (PSTN), the Internet, local area networks (LANs), wide area networks (WANs), and other corporate intranets, and may employ various data delivery systems such as cable, satellite, fiber optic lines, modems, and broadcast antennas, for example. A service provider (SP) 14 functions as a distributor of the content and a provider of communications services between the CP and the CC. In one embodiment, the SP may also function as a digital broadcast system (DBS), such as a satellite network, for example.

In one or more embodiments of the present invention, the CP of an ICA system may perform one or more of the following operations. The CP encrypts digital content with at least one key, transmits the encrypted digital content to at least one service provider, and requests creation of a secure channel for distribution of the encrypted digital content by the service provider. The CP also requests creation of a program to be sent on the channel (the program comprising the encrypted digital content) and installs at least one key at a content consumer for decrypting the program.

The SP of an ICA system according to embodiments of the present invention may perform one or more of the following operations. The SP receives encrypted digital content from at least one content provider, creates a secure channel for distribution of the encrypted digital content, creates a program for sending on the channel, and distributes the program.

The CC of an ICA system according to embodiments of the present invention may perform one or more of the following operations. The CC receives an announcement of program keys (which consists of at least keying material for that program such as a key and a time period for when the key is valid) to be distributed on a secure channel, receives a first key for gaining access to the secure channel, and receives a second key for decrypting the program data communicated over the secure channel. The CC also receives the program on the channel, and decrypts the encrypted digital content (the program) using the second key.

In any given ICA system, there may be multiple CPs, SPs, and CCs, in any combination. In one example, a single CP may provide content to a single SP, which in turn provides service to one or more CCs. In another example, a plurality of CPs may provide content to a single SP, which in turn provides service to one or more CCs. In yet another example, multiple CPs may provide content to multiple SPs. These SPs then provide service to one or more CCs.

This system may be employed in a variety of applications that distribute digital content such as multimedia streams to large numbers of receivers and provides a number of security features. The ICA system may allow or disallow individual destination networks from being able to decrypt network content. This is accomplished through the distribution of keying material only to receivers that are authorized and authenticated. The ICA system thereby supports encryption of network content "end-to-end" throughout the system. Some CCs may additionally employ content protection through the use of a trusted agent and also a trusted viewer. A trusted agent comprises system software that protects the channel key, and a trusted viewer comprises application software that protects the program key and controls how content is accessed and used on a CC. In the content-protection scenario, an ICA key server provides keys only to authorized and authenticated trusted viewers.

The ICA system comprises at least four characteristics that distinguish it from TV conditional access. First, the ICA system supports conditional access to content stored in network packets and files and is capable of executing on general purpose computer systems. Second, the ICA system works over a variety of network types and communications devices including Ethernet connections, modems, cable modems, asynchronous digital subscriber lines (ADSL), digital video broadcasting (DVB) systems, and advanced television standards committee (ATSC) systems, for example. Third, the ICA system may operate over multiple networks, not just multiple network types. For example, inter-network conditional access may be applied to a data flow that originates on an Ethernet connection, traverses one or more networks, including the Internet, and is received on an Ethernet connection or by a modem. Fourth, the ICA system also uses both multicast and unicast protocols and may operate over broadcast as well as point-to-point networks.

Definition of various terms used herein may be useful for understanding embodiments of the present invention. A channel carries keys for programs, and a program is an address or group of addresses having one or more keys assigned to them. The addresses may be unicast or multicast addresses. In one embodiment, each program may be carried out using a specific multicast address. Addresses may be grouped into programs with each address in the program carrying a media stream or package. For a particular program or set of programs, a CP may provide the encryption capabilities. Encryption processing may be offloaded from a SP to a CP for purposes of allowing the CP to control content security. A program may be content sent to one or more multicast addresses (e.g., a content channel) for a selected duration of time. A program comprises a series of logically related packages or a stream of data sent on a channel. A package comprises one or more files, which may be communicated repeatedly. A stream comprises one or more data packets having a temporal relationship between the packets. A program key is first announced to one or more CCs on a channel used for distributing program keys. Authorization, channel and program information are kept in a database under the control of the CP or SP owner of the channel. A database may be a set of data structures related to subscribers of channels and programs (e.g., CCs) and the data content they are authorized to receive.

The ICA system shown in Figure 1 provides service security and content security at least in part by creating trust relationships between the three subsystems. Creation of these trust relationships will be discussed below. Additionally, the system comprises three separate levels of security. First, a trusted group defined by access to a channel key allows access to a network service by application software of the content consumer (CC) that is authorized and authenticated by the owner of the service. The authorization and authentication may be of a particular computer system and/or user. Second, a member who is authorized and authenticated may gain access to a particular program key. Third, channel and program keys may be protected against access at the content consumer's computer by a trusted agent or trusted viewer that is authorized and authenticated to use specific channel and program keys without being able to directly read those keys. The use of trusted agents and trusted viewers are an optional content protection feature of the service.

II. Interfaces for Access and Content Control

Figure 2 is a diagram showing interfaces between a content provider (CP), a service provider (SP), and a content consumer (CC) according to the ICA system of Figure 1. These interfaces may be implemented by any appropriate means, such as Internet connections, satellite transmissions, PSTN back-channels, cables, and LANs, for example, although the invention is not limited in scope in this respect. One interface between a CP 10 and a SP 14 may be a request interface 20. Request interface 20 may be used to request mutual authentication of the CP and the SP and to request the distribution of channel and program keys. One interface between a SP 14 and a CC 12 may be a customer interface 22 where the CC may get the first key to a particular channel. First customer interface 22 may be used to request authorization and authentication of the CC by the SP, to assign channel keys, to assign program keys, and to report programs. One interface between a CP 10 and a CC 12 may be a second customer interface 24. Second customer interface 24 may be used to request mutual authentication of the CC and CP, to assign channel keys, to assign program keys, and to report programs. A first application tool interface 26 may be included in a CP 10 to initiate a launch of application software to control distribution of a program by the CP (e.g., such as a trusted server or player). A second application tool interface 28 may be included in a CC 12 to initiate a launch of application software, such as a trusted viewer, for example, for receiving and rendering a program that is being sent either multicast or unicast.

A first database interface 30 may be included to connect CP 10 with CP database 32. CP database 32 may be employed as necessary to store system data relating to channel members (e.g., users or CCs), channel keys, program keys, and authentication information (e.g., digital certificates as in a public key infrastructure (PKI), or other means). A second database interface 34 may be included to connect SP 14 with SP database 36. SP database 36 may be employed as necessary to store system data relating to channel members, channel keys, program keys and authentication information (e.g., digital certificates as in a public key infrastructure (PKI), or other means). CC 12 may also be coupled by third database interface 37 to a CC database 38, for storing information relating to available channels and programs. It is well known that databases such as these support a variety of operations for updating and querying information contained in them.

III. System Functions

In one embodiment, the ICA system provides functions to accomplish a particular task. Functions comprise multiple, sequential operations across at least one of the system interfaces shown in Figure 2. In the aggregate, the functions implement network and content security in an inter-network conditional access system for multicasting digital content. One embodiment of the present invention provides at least four functions: creating a channel for distribution of program keys, adding a member to the channel, removing a member from the channel, and distributing program keys on the channel. One embodiment of the present invention provides at least seven operations: authenticate/authorize, request a channel be established, assign channel keys, assign program keys, report program, database update, and database select.

A. Create a Channel for Distribution of Program Keys

Figure 3 is a diagram illustrating operations of a Create a Channel for Distribution of Program Keys function according to an embodiment of the present invention. This function requests an address from a SP by a CP for allocation as a channel on the SP's network. A channel comprises an address for sending program keys. Keys for programs may be distributed to a particular channel address. Channels may be created by a SP or a CP for the SP's network.

The Create a Channel for Distribution of Program Keys function may be implemented using the authenticate/authorize and request channel operations. First, SP 14 and CP 10 authenticate 50 each other, and an authorization check is made by the SP to confirm the rights of the CP. The CP then sends a request 52 to create a channel to the SP.

B. Adding a Member to the Channel

Either a SP or a CP may add a member (CC) to a channel to authorize a CC to provide a CC with a channel key and subsequently receive one or more program keys on the channel. Figure 4 is a diagram illustrating operations of the Adding a Member to the Channel function according to an embodiment of the present invention. This function may be used following execution of a successful Create a Channel for Distribution of Program Keys function to add a content consumer (CC) to the channel.

Adding a member to a channel owned by a SP may be implemented as follows. First, SP database 36 may be updated 54 by specifying to SP 14 the channel members and the authorization/authentication information to be modified along with the requested modifications. Next, SP 14 and CC 12 authenticate 56 each other, and SP performs an authorization check to confirm that the CC has rights to become a member of the channel. If successful, the SP adds a channel member 58 by sending channel information to the CC, thereby installing the channel key at the CC at 60. The CC then receives zero or more program keys on the channel and installs them at 62.

Figure 5 is a diagram illustrating operations of adding a member to a channel that is owned by a CP according to an embodiment of the present invention. This function may be used by the CP following execution of a successful Create Channel for Distribution of Program Keys functions to add content consumers (CCs) to the newly created channel, one at a time. In this embodiment, the SP does not have access to the unencrypted key to the channel nor to the program keys that are subsequently sent on the channel by the CP.

Adding a member to a channel owned by a CP may be implemented as follows. First, CP database 32 may be updated 64 by specifying to CP 10 the members, channel, and authorization/authentication information to be modified along with the requested modifications. Next, CP 10 and CC 12 authenticate 66 each other. Following a successful authorization check, the CP adds a channel 68 by sending the channel key to the CC, thereby installing the channel at the CC. The CP installs a channel key 70 at the CC for the new channel. The CP also installs a program key 72 for zero or more programs to be received on the new channel. Additional keys may also be added for zero or more programs.

C. Removing a Channel Member

Either a SP or a CP may remove a member from a channel it owns. Figure 6 is a diagram illustrating operations of removing a channel member from a channel owned by a SP according to an embodiment of the present invention. This function may be used by the SP to remove a CC from a channel. To accomplish this, the member's authorization (e.g., the selected CC) may be first removed from SP database 36 for this channel and then the keys for the channel may be changed for all other members of the group accessing the channel.

Removing a member from a channel function for an SP Channel may be implemented as follows. First, SP database 36 may be updated 74 by specifying to SP 14 the channel, member, and authorization/authentication information to be modified along with the requested modifications. Next, in one embodiment, the SP installs a new key 76 for the channel for all CCs subscribed to this channel except for the CC to be removed, thereby preventing the removed channel member from accessing the channel. In other embodiments, other well-known mechanisms for efficiently changing the keys at CC computers using multicast communications may be employed.

Figure 7 is a diagram illustrating operations of removing a member from a channel owned by a CP according to an embodiment of the present invention. This function may be used by the CP to remove a CC from a channel. To accomplish this, in one embodiment, the member (e.g., the selected CC) may be first removed from CP database 32 for this channel and then the keys for the channel may be changed for all other members of the group accessing the channel. Database operations to reflect the change may be authenticated and may be initiated by any party that is authorized by the CP or the SP. In other embodiments, other well-known mechanisms for efficiently changing the keys at CC computers using multicast communications may be employed.

Removing a member from a channel for a CP channel may be implemented at the CP as follows. First, CP database 32 may be updated 78 by specifying to CP 10 the members, channels, and authorization/authentication information to be modified along with the requested modifications. Next, in one embodiment, the CP may install a new key 80 for the channel for the channel for all CCs subscribed to this channel except for the CC to be removed, thereby preventing the removed channel member from accessing the channel. In other embodiments, other well-known mechanisms for efficiently changing the keys at CC computers using multicast communications may be employed.

D. Distributing Program Keys on a Channel

Figure 8 is a diagram illustrating operations of a distributing program keys on a channel function according to an embodiment of the present invention. This function may be used in the ICA system to securely distribute program keys over a multicast network.

The distribute program keys function may be implemented as follows. First, CP database 32 may be updated 80 by specifying to CP 10 the program-specific information such as channel, start time, and stop time to be modified along with the requested modifications. Alternatively, SP database

36 may be updated by SP 14 with this information. Next, CP 10 and SP 14 authenticate 82 each other, and an authorization check is performed for the CP by the SP. The CP requests one or more program keys be sent on a channel from the SP by a distribute program keys on a channel 84 operation from the SP. The SP distributes the program key or keys 86 to CC 12. The CC then installs keys 88 for the decrypting program on the CC. In one embodiment, the CC reports the program 90 by informing a billing system (not shown) at the CP or the SP that the program key or keys are being used and optionally that the content is being received, decrypted and viewed. In other embodiments, new programs may be reported to a billing system or subscription system included in the CP or SP. The communication from the CC to the CP or the SP may take place over a back channel (not shown).

IV. System Operations

One embodiment of the present invention provides at least seven operations to implement the system functions described above: authenticate/authorize, request channel, assign channel keys, assign program keys, report program, database update, and database select.

A. Authenticate/Authorize

Two way authentication is well known in the art. One security protocol commonly used on computer networks, such as the Internet, is Internet Protocol Security (IPSec), which has a protocol for authenticating senders and receivers. This protocol supports authentication using Diffie-Hellman and RSA and credentials such as the International Telecommunications Union (ITU) standard X.509 certificate infrastructure, a Public Key Infrastructure (PKI), or through a shared-key arrangement. These and other authentication means may be used by embodiments of the present invention.

In two way authentication, both parties such as Content Provider (CP) and Service Provider (SP), CP and Content Consumer (CC), or SP and CC, mutually authenticate each other at the start of a communications or information exchange session. In one-way authentication, however, there is no back-channel from one destination to the other as in many geo-synchronous satellite communications arrangements. One way authentication may be used in embodiments of the present invention through such means as "pre-shared" keys. For example, CP database 32 or CP database 36 may contain a shared secret key or a public key of a CC and data sent to the CC may be encrypted with this shared secret key or public key with the knowledge that only the CC who owns the corresponding secret key or private key portion of the public/private key pair will be able to decrypt the data. Similarly, the data may also be encrypted with the private key of the SP or CP and sent to the CC who has the corresponding public key of the public/private key pair of the sender (e.g., either the SP or the CP). In this way, the receiver will only be able to decrypt data sent by the particular sender. This may be used to avoid impersonation of the sender. The data that may be sent to the receiver may include a session key for a particular network stream of packets or a package of files that are being sent.

Authentication may be of two varieties, user authentication or platform authentication. An example of user authentication is when a person logs into a system using a password or even biometric data. The user may log in from different devices and be authenticated as a known user with known access rights to the system. An example of platform authentication is when a particular platform is authenticated using hardware and/or software features such as a unique identifier on a computer processor or a globally unique identifier on a version of the operating system that runs on the platform (such as a PC), or by a certificate, such as an X.509 certificate. For example, a caller-ID is a means of identifying an endpoint of a phone call, but the use of caller-ID does not identify which particular person is using the phone. On a general purpose computer such as a PC, however, there are various means for uniquely identifying the particular computer, such as processor identifier, or by various other means that are collectively referred to as a "dongle." When the platform is authenticated by means of a dongle, then some assurance is given that the platform serving as the source or receiver of data is the platform that is authorized to receive the data.

In the one embodiment, an authentication technique such as asymmetric public key cryptography (e.g., RSA or Diffie-Hellman) as described in various methods above may be used to encrypt or decrypt data that comprises a channel key. As described above, this channel key is used to encrypt zero or more program keys. In this embodiment, the channel key is called the Key Encrypting Key (KEK). The sender of the KEK has assurances that only an authenticated and authorized receiver can decrypt it and the receiver of a KEK can be assured that only an authenticated and authorized sender may have encrypted it. The KEK may encrypt a symmetric key that is used to encrypt program keys called traffic encrypting keys (TEKs). The TEKs may be used to encrypt data (e.g., program keys and program data) such as network packets that are sent to a group of one or more receivers. In one embodiment, the KEKs and TEKs may form a tree with a KEK corresponding to a subtree of receivers and TEKs corresponding to packet transmissions sent to receivers.

Figure 9 is a flow diagram illustrating an authentication/authorization operation according to an embodiment of the present invention. At block 100, a connection may be established between a two-party subset of the CP, SP or CC. At block 102, authentication may be performed using one of the methods described above. If authentication is successful at block 104, then the appropriate database is checked at block 105 to determine if the authenticated entity is authorized for the particular access. If authentication and authorization succeed at block 105, processing may performed, such as the transmission and/or the reception of data following the report of success shown in block 106. The error path of this processing occurs when the authentication/authorization operations of blocks 102 and 105 were not evaluated to be successful. This occurs when one of the parties did not successfully authenticate itself to the other or if the requesting entity was not authorized for the particular access. An authentication/authorization error may be processed in block 108, and in all cases, processing ceases at block 110.

Those skilled in the art of cryptography and network security will recognize that authentication may occur at the session level, such as at the commencement of communications and prior to the exchange of data among communicating endpoints, or it may occur at the packet level, where each packet is authenticated. When there are two communicating endpoints, the fact that the two endpoints share a secret key that is used for encrypting packets is implicit packet-level authentication since neither endpoint may impersonate the other. When there are more than two communicating endpoints, the situation becomes more complicated because any one of the endpoints may impersonate the sender when a symmetric key is used. There are well-known solutions to this problem using asymmetric cryptography. There also well-known solutions using the more efficient symmetric cryptography. Embodiments of the present invention may employ of any of these means.

B. Request Channel

The request channel operation obtains a multicast address from a SP's multicast address space for access to the SP's network. The request may result in a success or a failure. A failure may result when there are no more addresses to assign, for example. The request channel operation may be initiated as database operations performed against tables stored within the SP database and/or the CP database. A database update attempt may trigger an address allocation request. The outcome of this request determines the success or failure of the operation. When the request is successful, a new channel record may be added to the database. Results of the request channel may need to be kept consistent with the SP and CP databases.

Figure 10 is a flow diagram illustrating a content provider request channel operation according to an embodiment of the present invention. At block 120, a request may be made by the CP to the SP to get address parameters. A requested address range may be one parameter of the request; additional request parameters may include the duration of time that the address will be used for the channel. If the parameters are valid at block 122, the address may be obtained from the SP at block 124. An example of an invalid parameter is a specification of a time duration or address range that cannot be satisfied. Otherwise, a new request to get address parameters from the SP is made again at block 120. If the request is successful at block 126, then processing ends at block 128. If the SP fails to successfully obtain a channel, the error may be processed at block 130.

Figure 11 is a flow diagram illustrating a service provider request channel operation according to an embodiment of the present invention. The SP may wait for new channel requests. When a request is received from a CP at block 140, the request may be analyzed to determine its validity. If the request is valid at block 142, a multicast address may be allocated according to the request's parameters at block 144. If the request is invalid at block 142, the error may be processed at block 146 by reporting the error and returning to a wait state until the next CP request is received. An attempt may be made to allocate the address from a local or a hierarchical multicast address allocation server. If the attempt is unsuccessful at block 148, the error may be processed at block 146. Otherwise, an update to a channel database may occur at block 150 as a transaction against all copies of database tuples for the channel at the SP database and the CP database. At block 152, the success of the request may be reported to the requesting CP. SP request channel process then completes at block 154.

C. Assign Channel Keys

The assign channel keys operation installs a channel key for a content consumer (CC). A channel is a multicast address and a key for encrypting program keys that are sent to the channel address. A channel may carry one or more program keys encrypted with the channel key, and a program may be decrypted by a traffic encryption key (TEK). Information about channels may be represented as table entries in a subscriber database at the SP or the CP.

Figure 12 is a flow diagram illustrating content provider (CP) and service provider (SP) assign channel keys operations according to an embodiment of the present invention. A CP or SP adds a member to a channel by giving an address for the channel and the channel keys to the channel member following an authentication/authorization step. Once the channel key is generated, the key may be distributed to a channel member via unicast on a per channel member basis. The channel key is used to encrypt program keys that are sent to the channel address. The channel key may be communicated to the channel member by sending it directly to the channel member, by transmission on a unidirectional network such as a broadcast network, or may be distributed via a web request from the new channel member. A channel may use a trusted agent to prevent unauthorized copying of keys or agent software. A trusted agent protects the SP's keys using tamper-resistant techniques that prevent access to the keying material by application software other than the agent software that is authorized to use the key. A channel member is a CC who gets notice of the existence of a channel when it receives the address and is assigned keys for it.

A database update may be performed after an assign channel keys operation is completed and the member is successfully added to the channel. At block 160, an assign channel keys request may be obtained. At block 162, if the request is valid, then the requesting member may be authenticated/authorized at block 164. At block 166, if the authentication/authorization was successful, the member may be given keys to the channel at block 168. If the assign program keys operation succeeded, then the member was successfully added at block 170, the CP database (for CP processing) or the SP database (for SP processing) may be updated at block 172 to reflect the addition of the member to the channel. Processing is then complete at block 174. If an error is detected at blocks 162, 166, or 170, the error may be processed at block 176.

Figure 13 is a flow diagram illustrating a content consumer (CC) assign channel keys operation according to an embodiment of the present invention. If a CC is the target of the assign channel keys request (that is, a channel is being added to the channels accessible by this CC), then the processing shown in Figure 13 may be performed at the CC. At block 180, an assign channel keys request may be received from a SP or a CP. If the request is for this particular CC at block 182, the provider (either a CP or a SP) may be authenticated/authorized at block 184. If the authentication/authorization is successful at 186, the channel keys may be assigned and installed for use by the CC at block 188. If the channel key is to be tamper-resistant to prevent unauthorized duplication, a trusted agent may be installed on the content consumer (CC). The trusted agent handles the channel keys for the CC, and an SP or CP authenticates the trusted agent before providing a channel key to the CC. The CC will also authenticate the SP or CP and will only proceed if the SP or CP is authenticated. If the key assignment was successful at block 190, the CC monitors program keying material for the channel at block 192. Processing is then complete at block 194. If an error is detected at block 182, 186, or 190, the error may be processed at block 196.

D. Assign Program Keys

The assign program keys operation installs keys for a program. The key may be for a single address or multiple addresses. A program uses one or more keys to encrypt its data packet traffic. A program may require a trusted viewer for accessing the encrypted content that will protect the key and content from unauthorized use. In at least one embodiment of the present invention, the program key may be a tamper-resistant module.

Figure 14 is a flow diagram illustrating a service provider or content provider assign program keys operation according to an embodiment of the present invention. At block 300, a key request may be obtained by the SP or the CP to send program keys on a channel. A key request may be for a new set of program keys for an announcement, streams or package program, or to refresh the keys of a program to exclude certain members that have been removed from the channel. If the request is valid at block 302, one or more program keys may be generated at block 304. If the request is invalid at block 302, the error may be processed at block 306 and processing ends at block 308. An invalid request may be to assign keys or refresh the keys of a non-existing program or to remove a non-existent member from a channel. At block 310, the generated key may be sent to a channel member. Key distribution may be done on a sub-tree basis using multicast or on a single member basis. If more program keys are to distributed at block 312, then assign program keys processing continues with the next member at block 310. Otherwise, at block 314, the SP database may be updated for SP assign program keys processing, or the CP database may be updated for CP assign program keys processing. The distributed database update reflects the new system state existing after the end of successful assign program keys processing. SP or CP assign program keys processing ends at block 308.

Figure 15 is a flow diagram illustrating a content consumer assign program keys operation according to an embodiment of the present invention. At block 320, if a trusted viewer is not available on the CC, then a trusted viewer may be installed at block 322. A trusted viewer may be associated with a program. At block 324, an assign program keys request may be obtained. The request to assign keys to a program may be sent to a CC by a SP or CP either unicast or multicast. When the request is multicast, the assign program keys message may be received by a CC that is being removed as a channel member and thus that CC will not be able to decrypt the program key. Program keys may be assigned on a sub-tree basis using multicast or on a single member basis. At block 326, if the assign program keys request is meant for this CC, then one or more program keys may be updated at block 328. Program keys may be updated by refreshing the TEKs that are associated with the program. Otherwise, a new assign program keys request may again be obtained at block 324.

E. Report Program

The report program operation communicates when a CC joins or is receiving a program to a SP or a CP. An update of the SP database or the CP database occurs after receipt of the report. Parameters for the report may be obtained from an announcement, from a program key or channel key module, or may be viewer-specific. The report program message may be multicast or unicast. Implementation of the report program operation does not assume tethered consumption of content, and the report may be web based or updated periodically. Additionally, in one embodiment, a back channel interface may be used to convey the report information to either the SP database or the CP database.

V. Example of ICA System Processing

The ICA system may be used in one embodiment as follows. In a typical scenario for the ICA system, a channel may be created, at least one user may be added, and keys to a channel may be requested and distributed. When a channel is allocated and keys installed for that channel at one or more content consumer members of that channel, program keys can be sent to the members, whereby the program keys are encrypted in the channel key and sent to the channel address. Embodiments of the present invention accommodate various mechanisms for announcing, publicizing, notifying, sending and receiving program information such as distribution of digital information over packet networks. Besides adding users (which may be authenticated people or authenticated platforms), other operations may be used for removing users from the channel. The operations of adding or removing users, who are CC members of a channel, may be triggered by and may result in updates to a database management system operating at a SP or a CP. When a CC is removed from the channel, it may be necessary to change the channel key of all remaining CC members by assigning a new channel key to them.

Either through user intervention or as a result of an update to a database, a channel may be created by either the SP or the CP. The user, the platform, or the computer software that causes a channel to be created may be authenticated. As a result of channel creation, a database record may be created that includes information such as a channel name, a channel network address, channel policy information (e.g., identification of cryptographic algorithm, modes, key lengths, who may join the channel, etc.), and a CP or SP channel owner.

A CC (platform or user) may be added to a channel through user intervention or as a result of an update to a database at the SP or CP. The CC may be an authenticated platform or authenticated person. A database record may be created that includes information such as a CC name, a CC credentials, and other information. A CC receives a key to the channel upon being added to the ICA system. This channel key encrypts program keys, as described above. Each program may have its own traffic encryption key and even its own channel in a 'pay per view' embodiment. Alternatively, each channel may be used to carry keys for multiple programs as in a subscriber embodiment.

A group of content consumers (users or platforms) may receive multicast content that is 'pushed' to users as in Internet Protocol (IP) multicast networks. In this embodiment, multicast distribution of channel and program keys complements the multicast nature of the digital content distribution. Alternatively, individual users may request digital content be delivered directly to them in a unicast embodiment of the present invention.

If the digital content is delivered unicast to the CC, such as on networks that do not support multicast operation, then the keying material may also be requested and received unicast, such as channel and program keys that are 'pulled' to the CC by a web browser application. In both cases of multicast and unicast distribution, there is a common structure of keying material for channel and program keys. The operations described herein are applicable to both the unicast and multicast cases.

In both the unicast and multicast cases, there is a corresponding operation to add information about the channel, program, or CC to the CP or SP database. The CP database may be updated when the CP maintains the security associations (SAs) for the program as, for example, when a company is sending proprietary information to its offices using a network service provider and the program in question is not to be shared with the network service provider (SP). In either case of a CP or SP database update, an association may be formed between the channel, one or more programs, and one or more CC members.

Members may need to be removed from a channel when, for example, their subscription expires to channel content. This operation may be accomplished by multicast or unicast distribution of new channel keys to the remaining members of the channel. In the case of multicast, there are efficient means of distributing keys to large numbers of channel members that are logarithmic in complexity and which do not require unicast exchanges between the key management center in the CP or SP and individual members. Those skilled in the art of multicast networking will recognize that a user may be added or removed from a channel with logarithmic message, storage and processing complexity when a tree or hierarchical structure is used. Embodiments of the present invention use hierarchical data structures for managing keys to change the keys of members after a member is removed from a channel or before a new member is added to the channel. The removal of a user may be accompanied by an update the database system in the CP or the SP to remove any association with the user and the channel or program.

In the preceding description, various aspects of the present invention have been described. For purposes of explanation, specific numbers, systems and configurations were set forth in order to provide a thorough understanding of the present invention. However, it is apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well-known features were omitted or simplified in order not to obscure the present invention.

Embodiments of the present invention may be implemented in hardware or software, or a combination of both. However, embodiments of the invention may be implemented as computer software executing on programmable systems comprising at least one processor, a data storage system (including volatile and non-volatile memory and/or storage elements), at least one input device, and at least one output device. One or more of service providers (SPs), content providers (CPs), and content consumers (CCs) may be implemented as programmable systems. Programmable software may be applied to input data to perform the functions described herein and generate output information. The output information may be applied to one or more output devices, in known fashion. For purposes of this application, a processing system includes any system that has a processor, such as, for example, a digital signal processor (DSP), a microcontroller, an application specific integrated circuit (ASIC), or a microprocessor.

The programs may be implemented in a high level procedural or object oriented programming language to communicate with a processing system. The programs may also be implemented in assembly or machine language, if desired. In fact, the invention is not limited in scope to any particular programming language. In any case, the language may be a compiled or interpreted language.

The programs may be stored on a storage media or device (e.g., hard disk drive, floppy disk drive, read only memory (ROM), CD-ROM device, flash memory device, digital versatile disk (DVD), or other storage device) readable by a general or special purpose programmable processing system, for configuring and operating the processing system when the storage media or device is read by the processing system to perform the procedures described herein. Embodiments of the invention may also be considered to be implemented as a machine-readable storage medium, configured for use with a processing system, where the storage medium so configured causes the processing system to operate in a specific and predefined manner to perform the functions described herein.

An example of one such type of processing system is shown in Figure 16. Sample system 400 may be used, for example, to execute the processing for methods employed by the content provider, service provider, or content consumer, in accordance with the present invention, such as the embodiment described herein. Sample system 400 is representative of processing systems based on the PENTIUM®, PENTIUM® Pro, PENTIUM® II, PENTIUM® III, and CELERON™ microprocessors available from Intel Corporation, although other systems (including personal computers (PCs) having other microprocessors, engineering workstations, set-top boxes and the like) may also be used. In one embodiment, sample system 400 may be executing a version of the WINDOWS™ operating system available from Microsoft Corporation, although other operating systems and graphical user interfaces, for example, may also be used.

Figure 16 is a block diagram of a system 400 of one embodiment of the present invention. The computer system 400 includes a processor 402 that processes data signals. The processor 402 may be a complex instruction set computer (CISC) microprocessor, a reduced instruction set computing (RISC) microprocessor, a very long instruction word (VLIW) microprocessor, a processor implementing a combination of instruction sets, or other processor device, such as a digital signal processor, for example.

Figure 16 shows an example of an embodiment of the present invention implemented as a single processor system 400. However, it is understood that embodiments of the present invention may alternatively be implemented as systems having multiple processors. Processor 402 may be coupled to a processor bus 404 that transmits data signals between processor 402 and other components in the system 400.

System 400 includes a memory 406. Memory 406 may be a dynamic random access memory (DRAM) device, a static random access memory (SRAM) device, or other memory device. Memory 406 may store instructions and/or data represented by data signals that may be executed by processor 402. The instructions and/or data may comprise code for performing any and/or all of the techniques of the present invention. Memory 406 may also contain additional software and/or data (not shown). A cache memory 408 may reside inside processor 402 that stores data signals stored in memory 406. Cache memory 408 in this embodiment speeds up memory accesses by the processor by taking advantage of its locality of access. Alternatively, in another embodiment, the cache memory may reside external to the processor.

A bridge/memory controller 410 may be coupled to the processor bus 404 and memory 406. The bridge/memory controller 410 directs data signals between processor 402, memory 406, and other components in the system 400 and bridges the data signals between processor bus 404, memory 406, and a first input/output (I/O) bus 412. In some embodiments, the bridge/memory controller provides a graphics port for coupling to a graphics controller 413. In this embodiment, graphics controller 413 interfaces to a display device (not shown) for displaying images rendered or otherwise processed by the graphics controller 413 to a user.

First I/O bus 412 may comprise a single bus or a combination of multiple buses. First I/O bus 412 provides communication links between components in system 400. A network controller 414 may be coupled to the first I/O bus 412. The network controller links system 400 to a network that may include a plurality of processing systems (not shown in Figure 16) and supports communication among various systems. The network of processing systems may comprise a local area network (LAN), a wide area network (WAN), the Internet, or other network. In some embodiments, a display device controller 416 may be coupled to the first I/O bus 412. The display device controller 416 allows coupling of a display device to system 400 and acts as an interface between a display device (not shown) and the system. The display device may comprise a television set, a computer monitor, a flat panel display, or other suitable display device. The display device receives data signals from processor 402 through display device controller 416 and displays information contained in the data signals to a user of system 400.

In some embodiments, camera 418 may be coupled to the first I/O bus to capture live events. Camera 418 may comprise a digital video camera having internal digital video capture hardware that translates a captured image into digital graphical data. The camera may comprise an analog video camera having digital video capture hardware external to the video camera for digitizing a captured image. Alternatively, camera 418 may comprise a digital still camera or an analog still camera coupled to image capture hardware. A second I/O bus 420 may comprise a single bus or a combination of multiple buses. The second I/O bus 420 provides communication links between components in system 400. A data storage device 422 may be coupled to the second I/O bus 420. The data storage device 422 may comprise a hard disk drive, a floppy disk drive, a CD-ROM device, a flash memory device, or other mass storage device. Data storage device 422 may comprise one or a plurality of the described data storage devices.

A keyboard interface 424 may be coupled to the second I/O bus 420. Keyboard interface 424 may comprise a keyboard controller or other keyboard interface device. Keyboard interface 424 may comprise a dedicated device or may reside in another device such as a bus controller or other controller device. Keyboard interface 424 allows coupling of a keyboard to system 400 and transmits data signals from a keyboard to system 400. A user input interface 425 may be coupled to the second I/O bus 420. The user input interface may be coupled to a user input device, such as a mouse, joystick, or trackball, for example, to provide input data to the computer system. Audio controller 426 may be coupled to the second I/O bus 420. Audio controller 426 operates to coordinate the recording and playback of audio signals. A bus bridge 428 couples first I/O bridge 412 to second I/O bridge 420. The bus bridge operates to buffer and bridge data signals between the first I/O bus 412 and the second I/O bus 420.

Embodiments of the present invention are related to the use of the system 400 to provide a portion of an inter-network conditional access system. According to one embodiment, provision of content provider, service provider, and/or content consumer operations may be performed by the system 400 in response to processor 402 executing sequences of instructions in memory 404. Such instructions may be read into memory 404 from another computer-readable medium, such as data storage device 422, or from another source via the network controller 414, for example. Execution of the sequences of instructions causes processor 402 to perform content provider, service provider, and/or content consumer operations according to embodiments of the present invention. In an alternative embodiment, hardware circuitry may be used in place of or in combination with software instructions to implement embodiments of the present invention. Thus, the present invention is not limited to any specific combination of hardware circuitry and software.

The elements of system 400 perform their conventional functions well-known in the art. In particular, data storage device 422 may be used to provide long-term storage for the executable instructions and data structures for embodiments of methods of performing content provider, service provider, and/or content consumer operations in accordance with the present invention, whereas memory 406 is used to store on a shorter term basis the executable instructions of embodiments of the methods for performing content provider, service provider, and/or content consumer operations in accordance with the present invention during execution by processor 402.

A system that unifies network security and application/content security in a single system to protect a service provider's service and to secure a content provider's content has been described.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the inventions pertains are deemed to lie within the spirit and scope of the invention.

CLAIMS

What is claimed is:

1. An inter-network conditional access system comprising:

at least one content provider to provide digital content; and

at least one service provider, communicatively coupled to the at least one content provider, to securely receive the digital content from the at least one content provider and to securely distribute the digital content; and

wherein the at least one content provider and the at least one service provider create a first relationship of trust between the at least one content provider and the at least one service provider.

2. The inter-network conditional access system of claim 1, further comprising:

at least one content consumer, communicatively coupled to the at least one service provider, to securely receive the digital content from the at least one service provider and to securely consume the digital content; and

wherein the at least one content consumer and the at least one service provider create a second relationship of trust between the at least one content consumer and the at least one service provider.

3. The inter-network conditional access system of claim 2, wherein the at least one content consumer is communicatively coupled to the at least one content provider; and

wherein the at least one content consumer and the at least one content provider create a third relationship of trust between the at least one content consumer and the at least one content provider.

4. The inter-network conditional access system of claim 1, wherein the at least one content provider is communicatively coupled to the at least

one service provider by a first interface, the first interface being used to perform at least one of authentication/authorization, request channel, and assign channel keys operations.

5. The inter-network conditional access system of claim 2, wherein the at least one service provider is communicatively coupled to the at least one content consumer by a second interface, the second interface being used to perform at least one of authentication/authorization, assign channel keys, assign program keys, and report program operations.

6. The inter-network conditional access system of claim 3, wherein the at least one content provider is communicatively coupled to the at least one content consumer by a third interface, the third interface being used to perform at least one of authentication/authorization, assign channel keys, assign program keys, and report program operations.

7. The inter-network conditional access system of claim 1, further comprising a first database coupled to the at least one service provider to store information relating to at least one of channels, members of channels, and multicast addresses of channels.

8. The inter-network conditional access system of claim 1, further comprising a second database coupled to the at least one content provider to store information relating to at least one of channels, members of channels, programs, and authorization/authentication information.

9. The inter-network conditional access system of claim 2, further comprising a third database coupled to the at least one content consumer to store information relating to at least one of channels and programs.

10. The inter-network conditional access system of claim 2, wherein the at least one content consumer comprises a trusted viewer for processing the digital content received from the at least one service provider.

11. The inter-network conditional access system of claim 2, wherein the digital content is encrypted by the at least one content provider and decrypted by the at least one content consumer.

12. The inter-network conditional access system of claim 1, wherein the system operates in a multicast network environment.

13. In an inter-network conditional access system having at least one service provider and at least one content consumer, a method of providing content comprising:

encrypting digital content with at least one key;

transmitting the encrypted digital content to the at least one service provider;

requesting creation of a secure channel for distribution of the encrypted digital content by the at least one service provider;

requesting creation of a program to be sent on the channel, the program comprising the encrypted digital content; and

installing the at least one key at the at least one content consumer for decrypting the program.

14. The method of claim 13, further comprising performing authentication of at least one of the at least one service provider and the at least one content consumer.

15. The method of claim 13, further comprising adding the at least one content consumer as a member to the channel.

16. The method of claim 15, further comprising removing the at least one content consumer as a member from the channel.

17. In an inter-network conditional access system having at least one content provider and at least one content consumer, a method of providing service comprising:

receiving encrypted digital content from the at least one content provider;

creating a secure channel for distribution of the encrypted digital content;

creating at least one key for decrypting the encrypted digital content sent on the channel, the program comprising the encrypted digital content; and

sending the at least one key to the at least one content consumer.

18. The method of claim 17, further comprising adding the at least one content consumer as a member to the channel.

19. The method of claim 17, further comprising removing the at least one content consumer as a member from the channel.

20. The method of claim 17, further comprising performing authentication of at least one of the at least one content provider and the at least one content consumer.

21. In an inter-network conditional access system having at least one content provider and at least one service provider, a method of consuming content comprising:

receiving first and second keys distributed on a secure channel, the first key for gaining access to the secure channel and the second key for decrypting the program communicated over the secure channel, the program comprising encrypted digital content, and the first key being encrypted by the second key;

decrypting the second key using the first key; and

decrypting the encrypted digital content using the decrypted second key.

22. The method of claim 21, further comprising viewing the decrypted digital content with a trusted viewer.

23. The method of claim 21, further comprising reporting the decrypting and viewing to at least one of the at least one service provider and the at least one content provider.

24. The method of claim 21, further comprising performing authentication of at least one of the at least one service provider and the at least one content provider.

25. An article comprising a machine readable medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions cause a content provider, in an inter-network conditional access system having at least one service provider and at least one content consumer, to:

encrypt digital content with at least one key;

transmit the encrypted digital content to the at least one service provider;

request creation of a secure channel for distribution of the encrypted digital content by the at least one service provider;

request creation of a program to be sent on the channel, the program comprising the encrypted digital content; and

install the at least one key at the at least one content consumer for decrypting the program.

26. An article comprising a machine readable medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions cause a service provider, in an inter-network conditional access system having at least one content provider and at least one content consumer, to:

receive encrypted digital content from the at least one content provider;

create a secure channel for distribution of the encrypted digital content;

create at least one key for decrypting the encrypted digital content sent on the channel, the program comprising the encrypted digital content; and

send the at least one key to the at least one content consumer.

27. An article comprising a machine readable medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions cause a content consumer, in an inter-network conditional access system having at least one content provider and at least one service provider to:

receive first and second keys distributed on a secure channel, the first key for gaining access to the secure channel and the second key for decrypting the program communicated over the secure channel, the program comprising encrypted digital content, and the first key being encrypted by the second key;

decrypt the second key using the first key; and

decrypt the encrypted digital content using the decrypted second key.

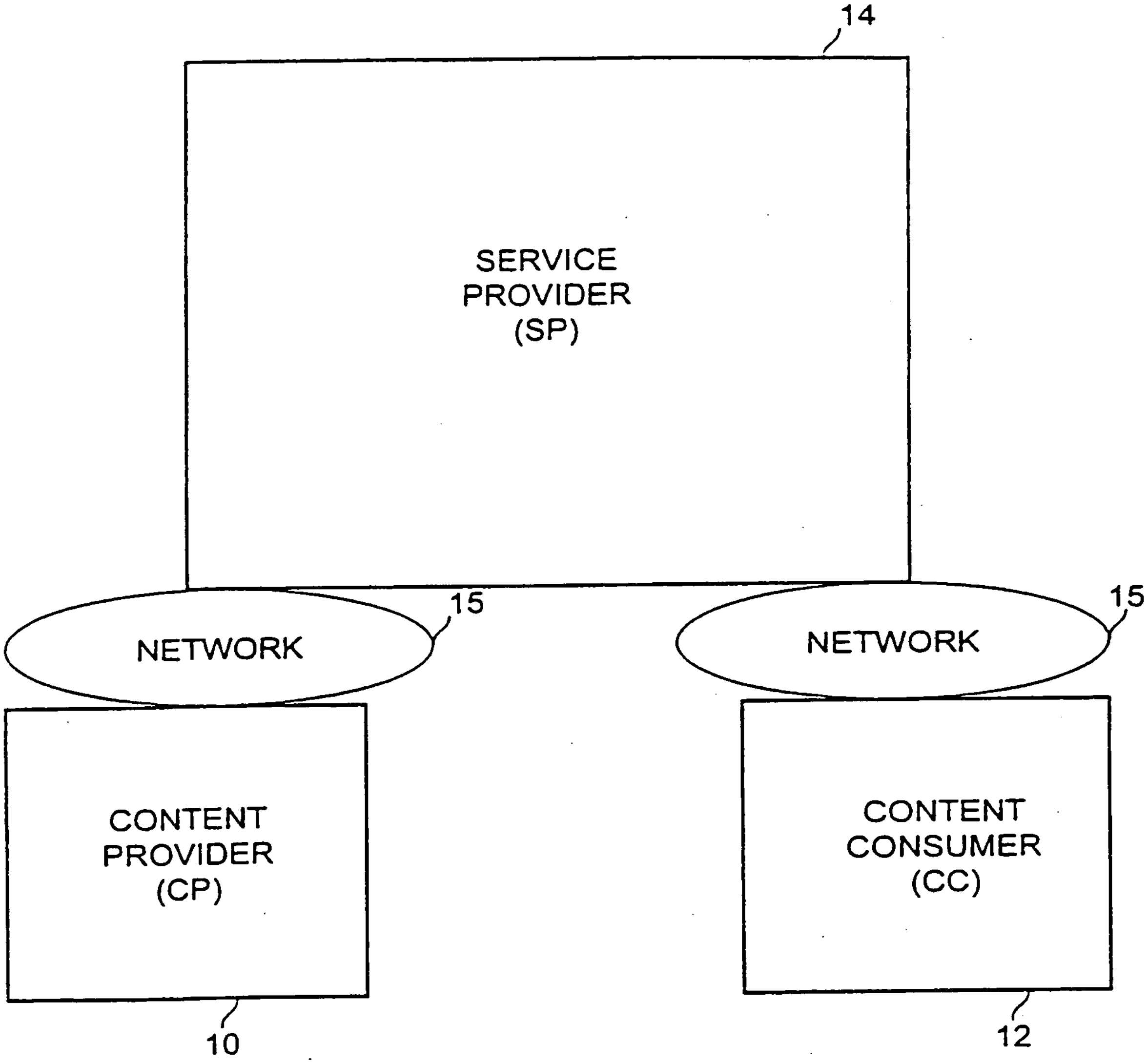

14
SERVICE PROVIDER (SP)
15
NETWORK
15
NETWORK
CONTENT PROVIDER (CP)
CONTENT CONSUMER (CC)
10
12

Figure 1

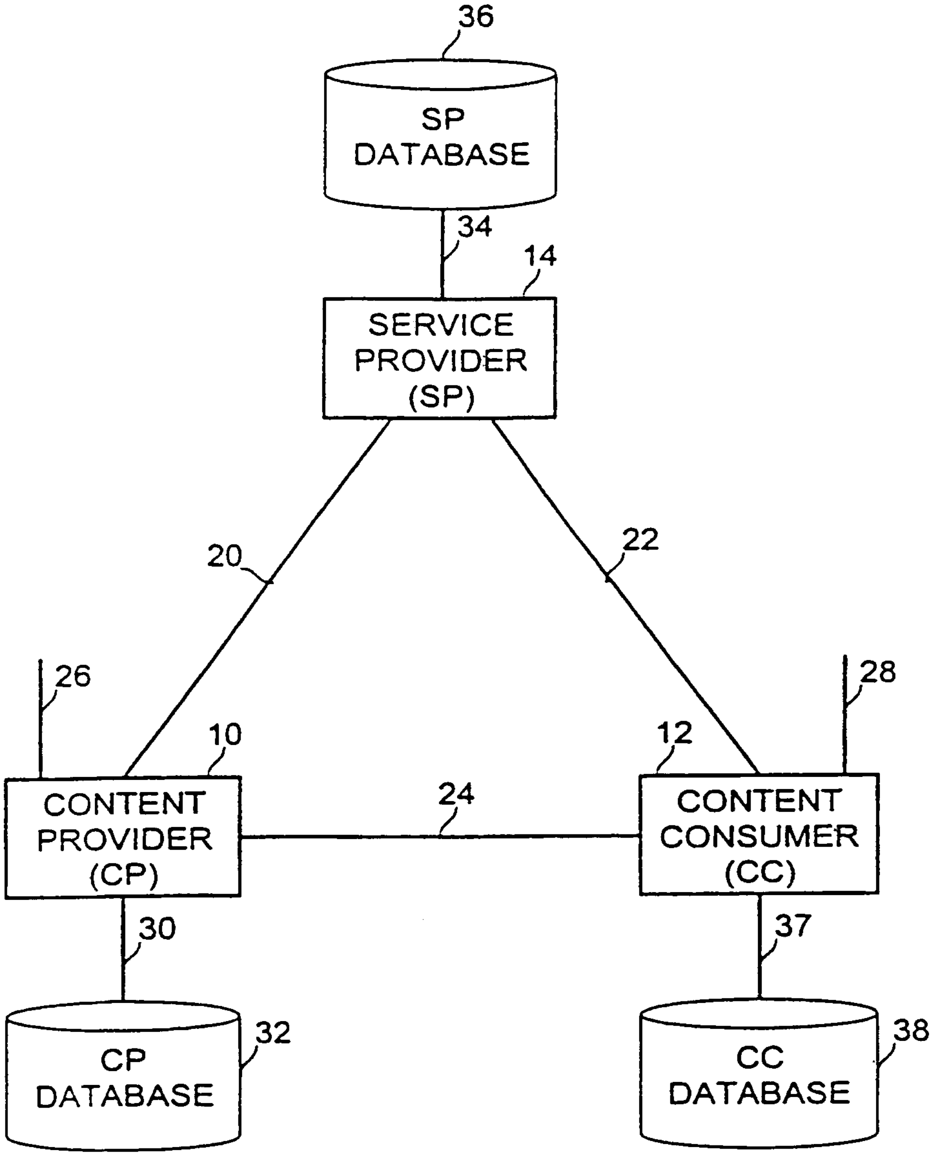

36
SP DATABASE
34
14
SERVICE PROVIDER (SP)
20
22
26
28
10
12
24
CONTENT PROVIDER (CP)
CONTENT CONSUMER (CC)
30
37
32
38
CP DATABASE
CC DATABASE

Figure 2

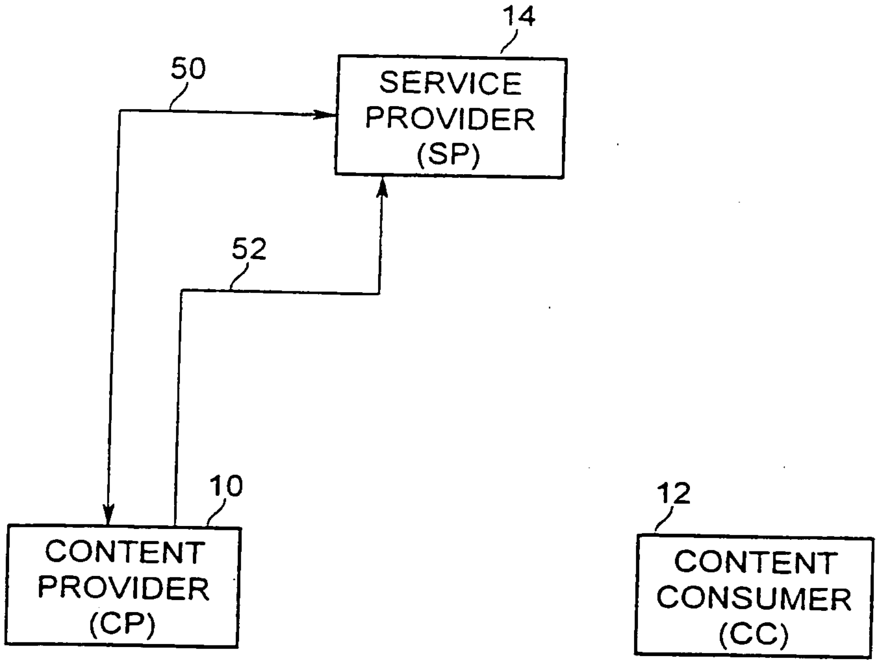

14
SERVICE PROVIDER (SP)
50
52
10
CONTENT PROVIDER (CP)
12
CONTENT CONSUMER (CC)

Figure 3

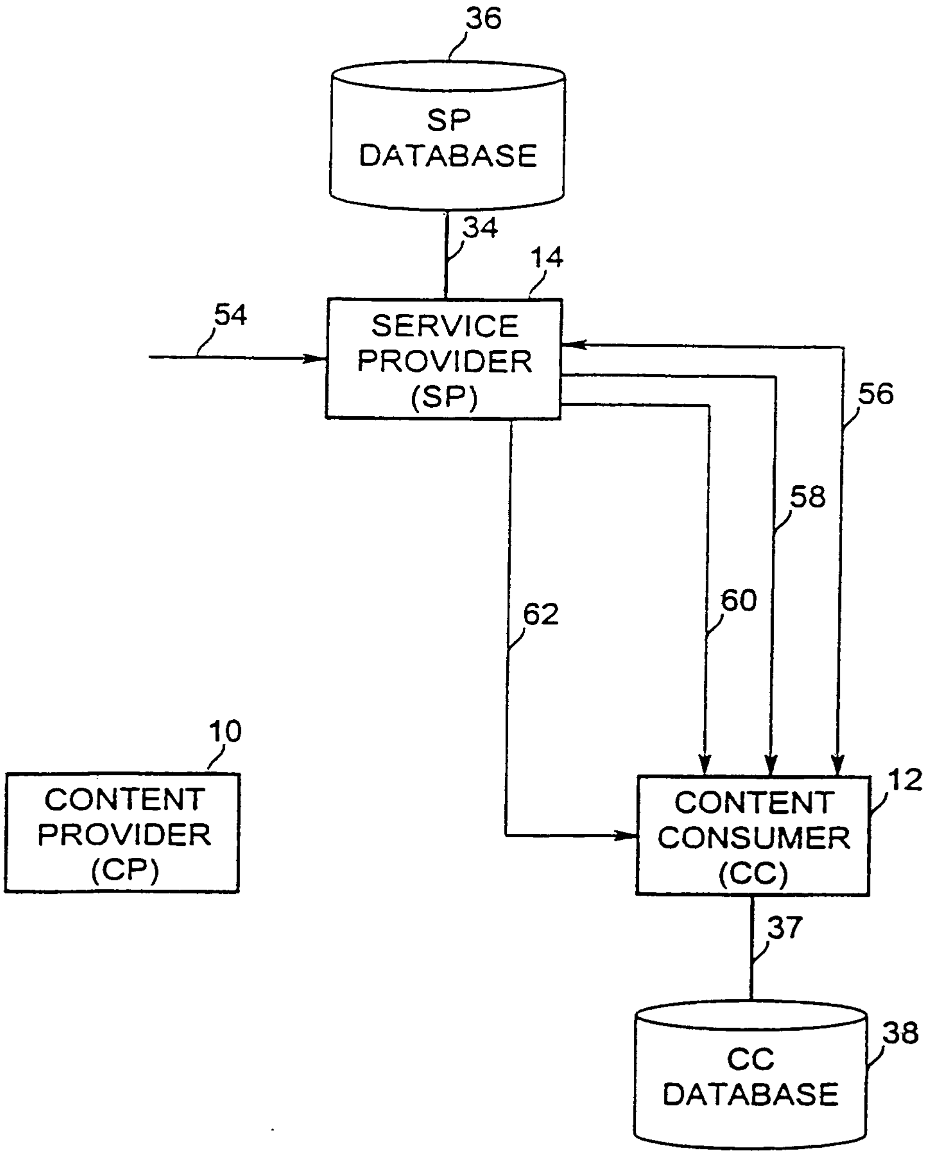

36
SP DATABASE
34
14
54
SERVICE PROVIDER (SP)
56
58
60
62
10
CONTENT PROVIDER (CP)
CONTENT CONSUMER (CC)
12
37
CC DATABASE
38

Figure 4

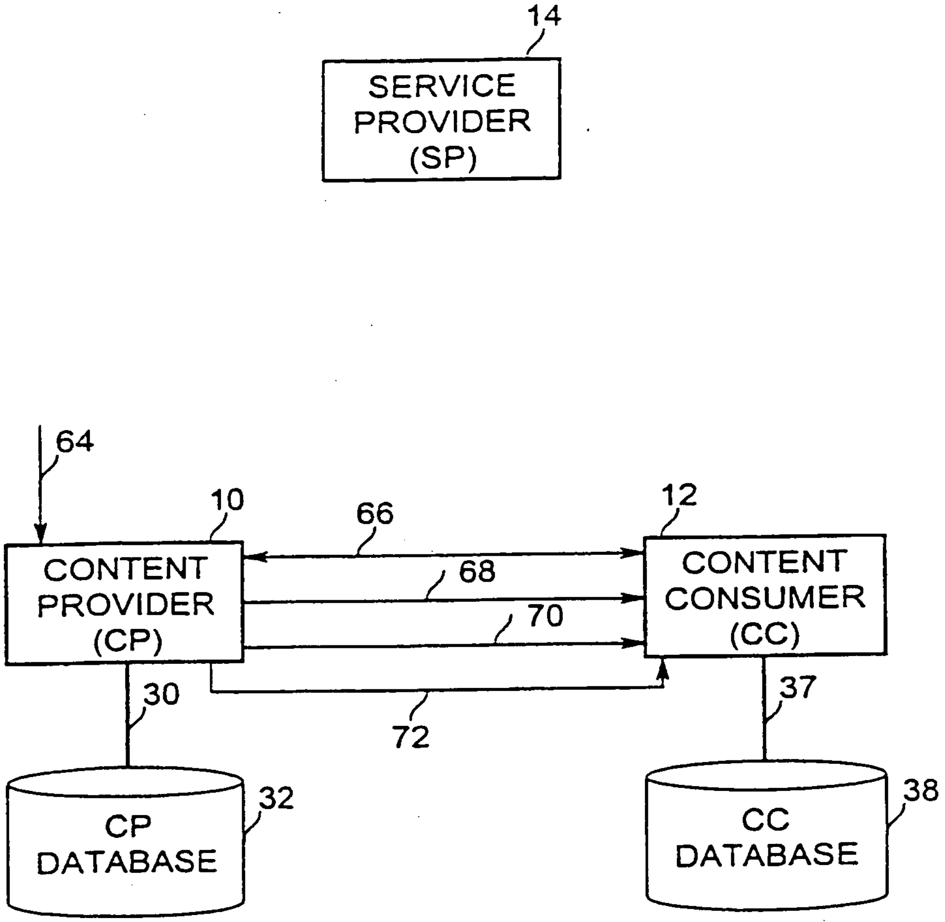

14
SERVICE PROVIDER (SP)
64
10
CONTENT PROVIDER (CP)
66
68
70
72
12
CONTENT CONSUMER (CC)
30
32
CP DATABASE
37
38
CC DATABASE

Figure 5

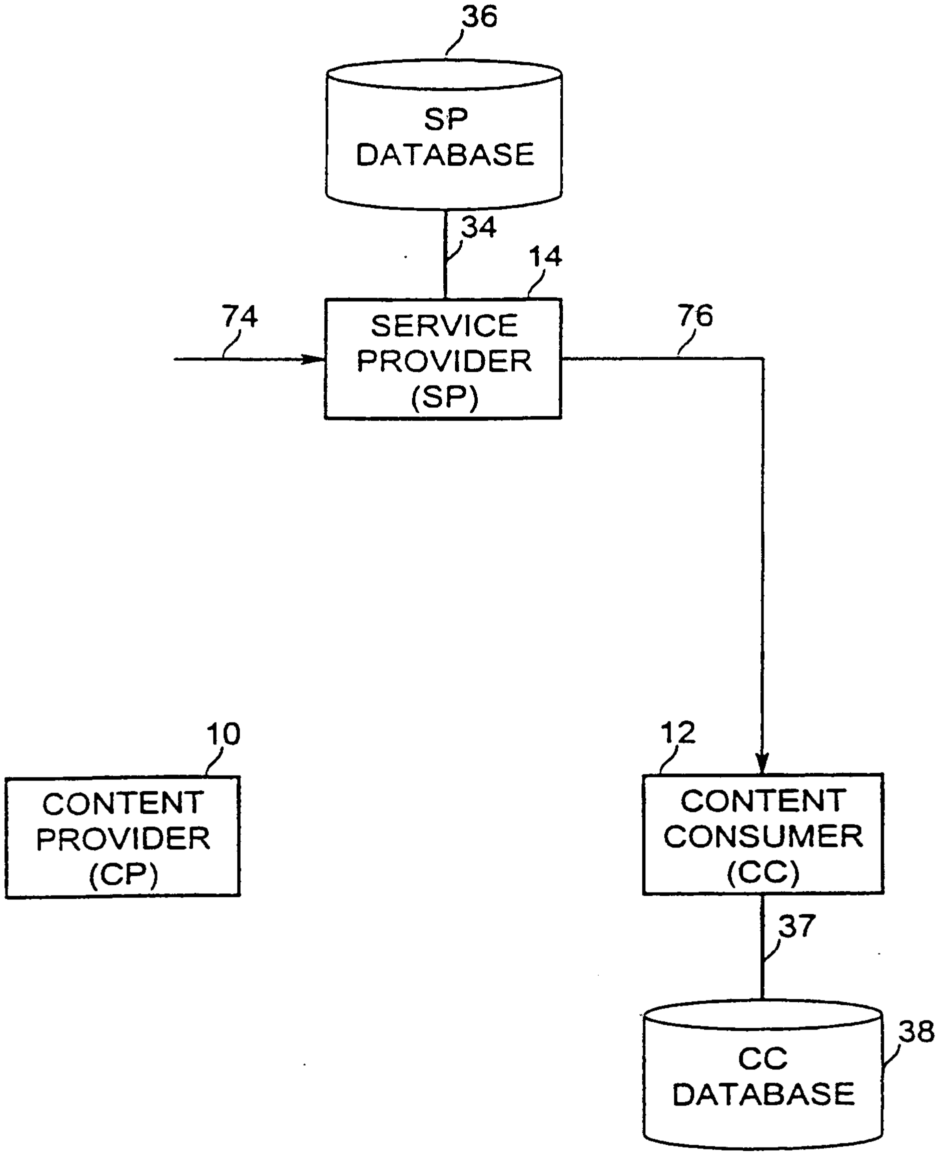

36
SP DATABASE
34
14
74
SERVICE PROVIDER (SP)
76
10
CONTENT PROVIDER (CP)
12
CONTENT CONSUMER (CC)
37
38
CC DATABASE

Figure 6

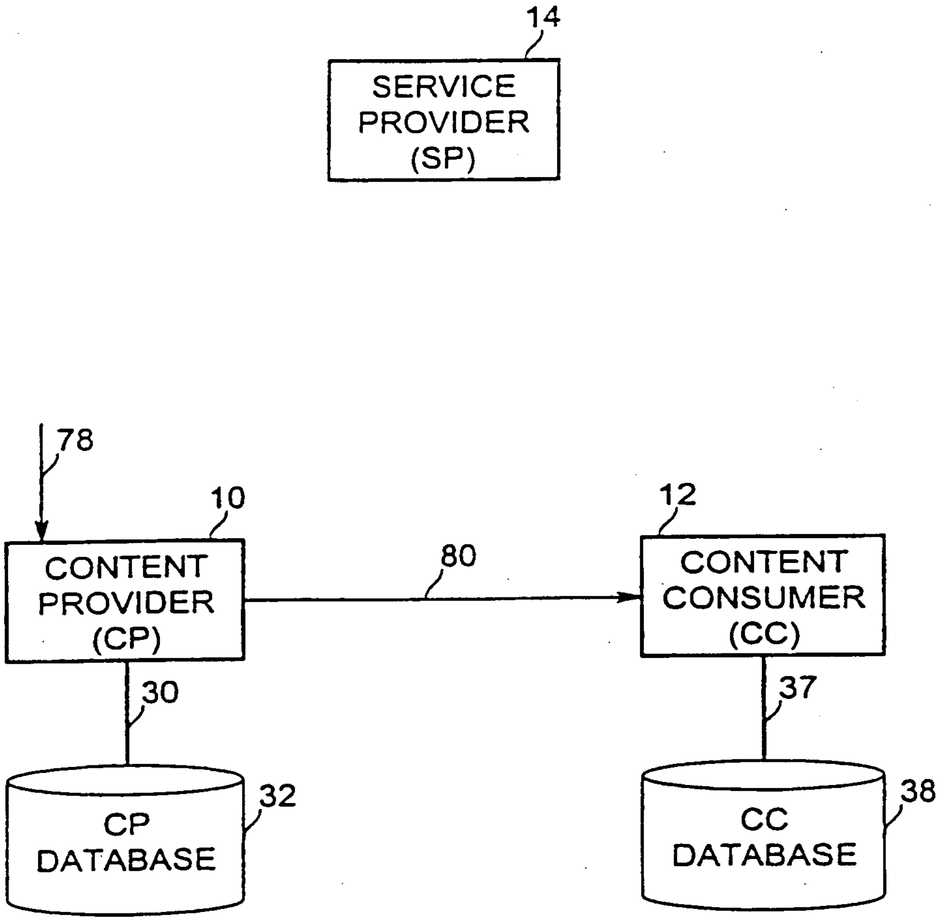

14
SERVICE PROVIDER (SP)
78
10
CONTENT PROVIDER (CP)
80
12
CONTENT CONSUMER (CC)
30
37
32
CP DATABASE
38
CC DATABASE

Figure 7

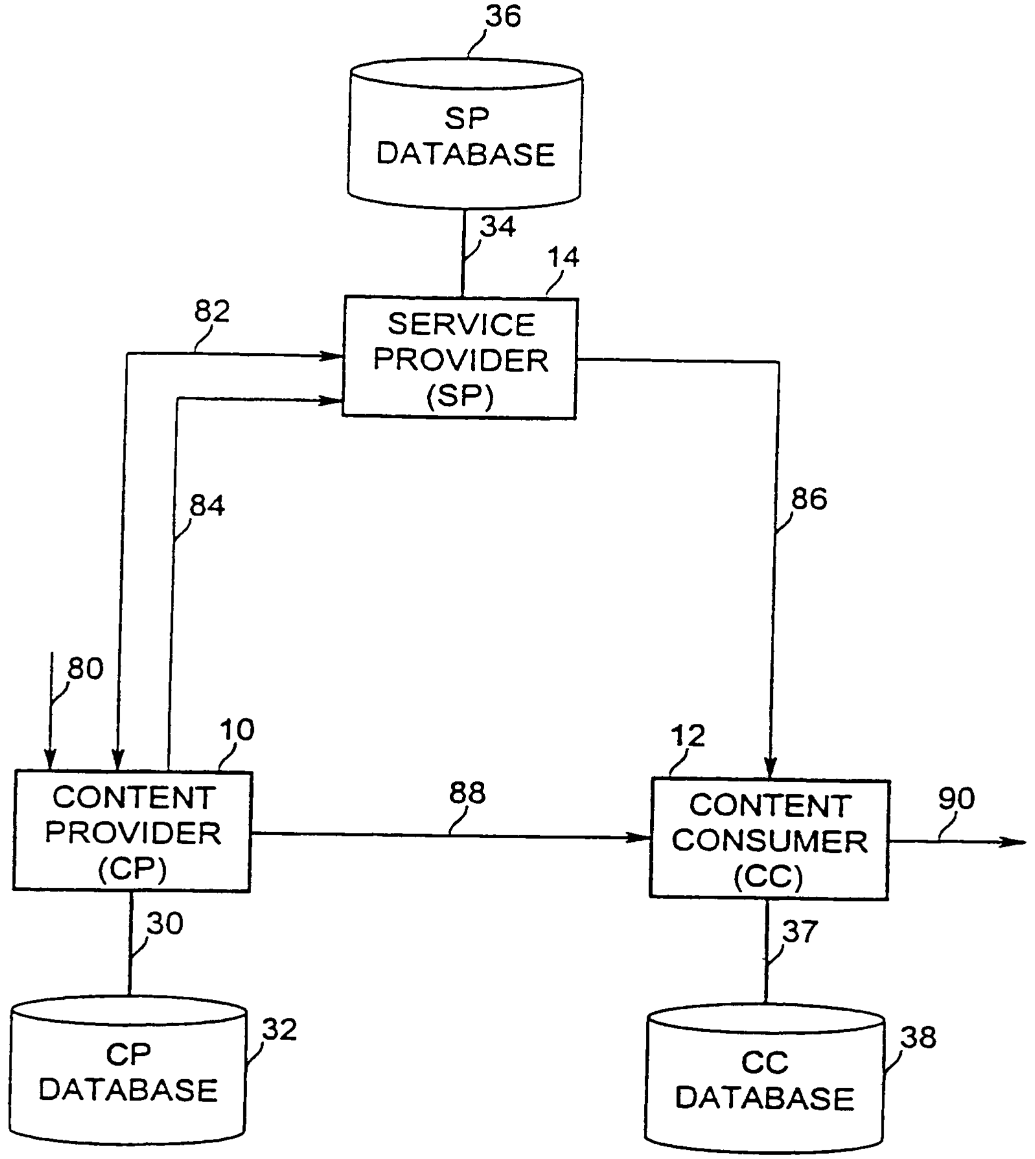

36
SP DATABASE
34
14
SERVICE PROVIDER (SP)
82
84
86
80
10
CONTENT PROVIDER (CP)
88
12
CONTENT CONSUMER (CC)
90
30
CP DATABASE
32
37
CC DATABASE
38

Figure 8

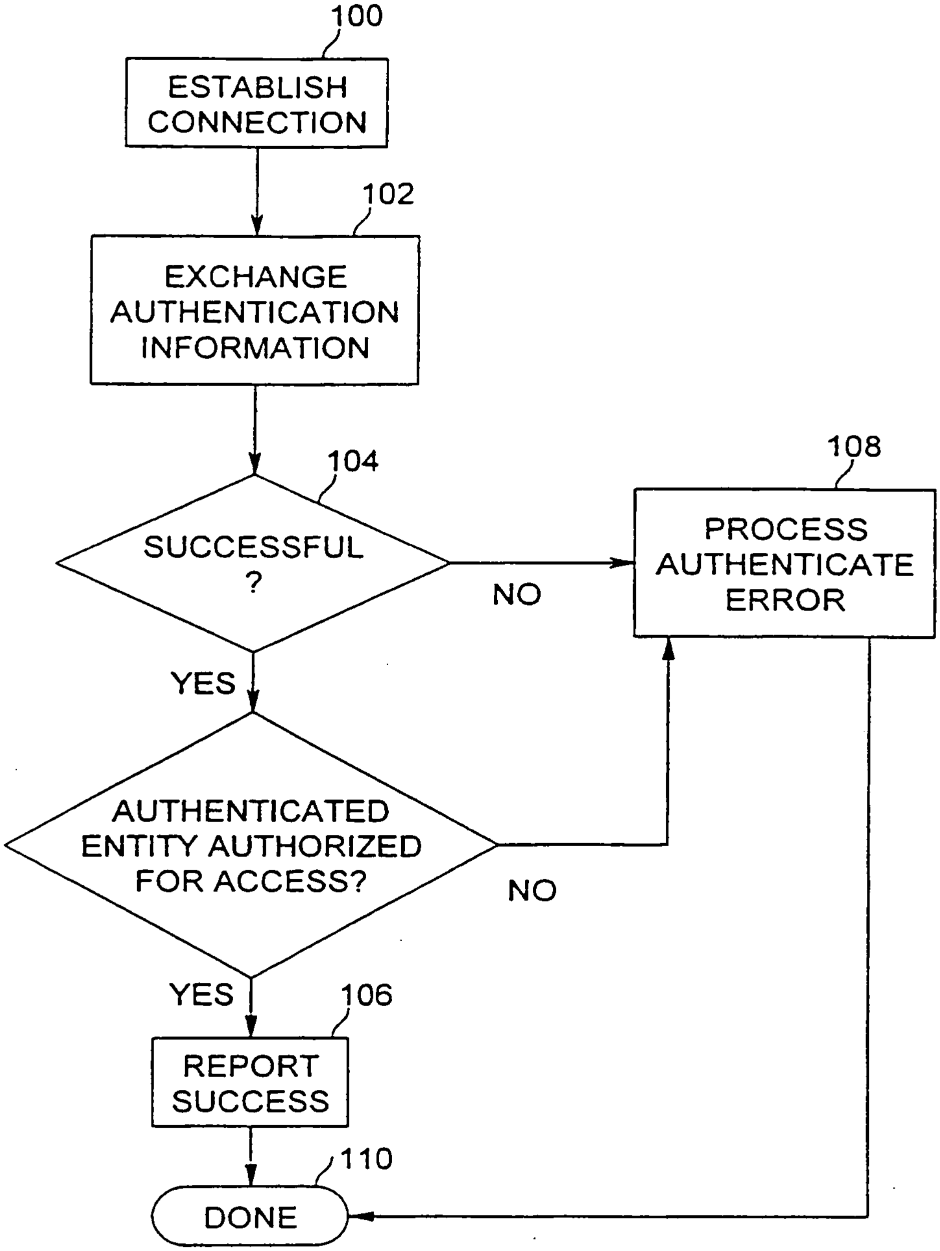

100
ESTABLISH CONNECTION
102
EXCHANGE AUTHENTICATION INFORMATION
104
SUCCESSFUL ?
NO
108
PROCESS AUTHENTICATE ERROR
YES
AUTHENTICATED ENTITY AUTHORIZED FOR ACCESS?
NO
YES
106
REPORT SUCCESS
110
DONE

Figure 9

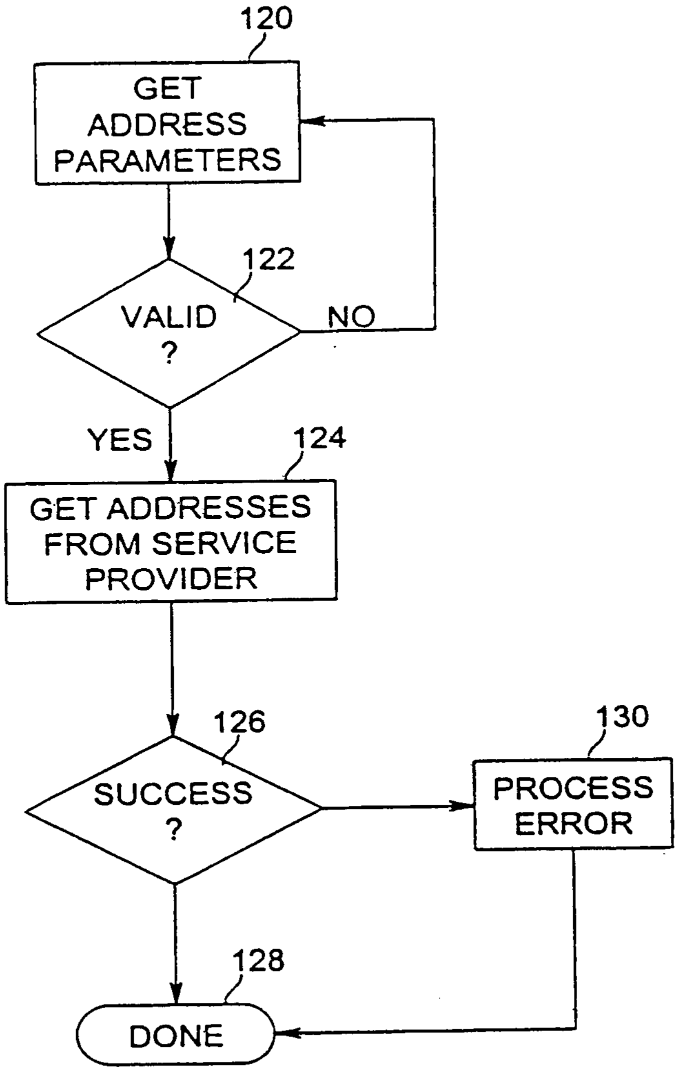

120
GET ADDRESS PARAMETERS
122
VALID ?
NO
YES
124
GET ADDRESSES FROM SERVICE PROVIDER
126
SUCCESS ?
130
PROCESS ERROR
128
DONE

Figure 10

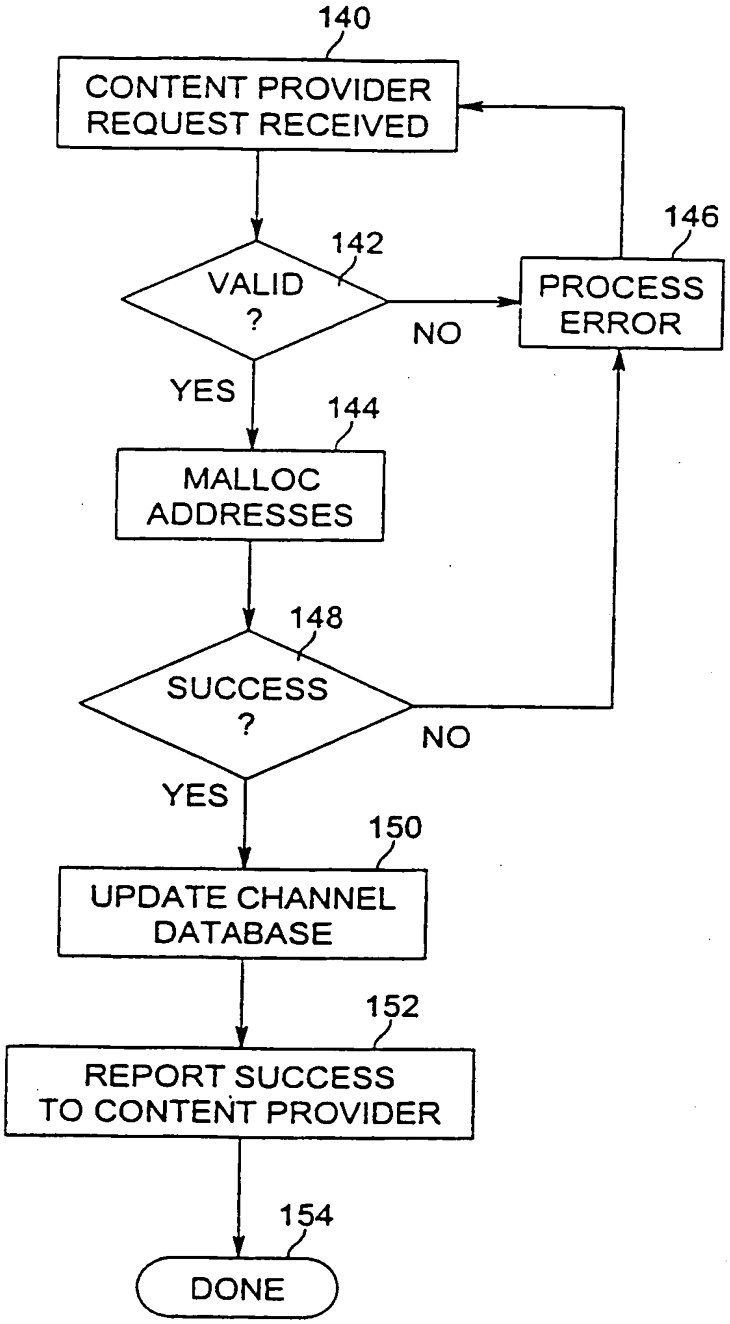

140
CONTENT PROVIDER REQUEST RECEIVED
142
VALID ?
NO
YES
146
PROCESS ERROR
144
MALLOC ADDRESSES
148
SUCCESS ?
NO
YES
150
UPDATE CHANNEL DATABASE
152
REPORT SUCCESS TO CONTENT PROVIDER
154
DONE

Figure 11

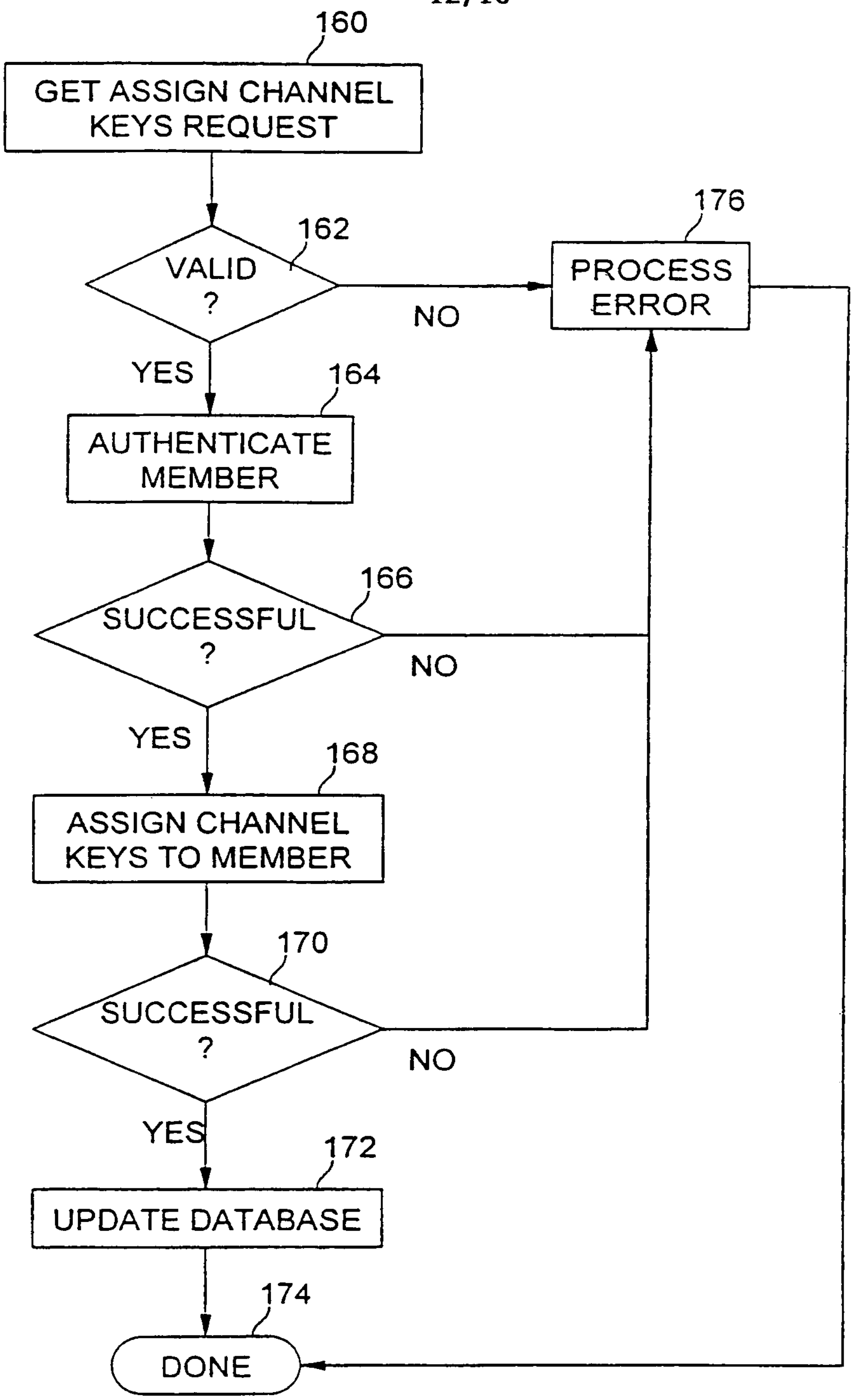

160
GET ASSIGN CHANNEL KEYS REQUEST
162
VALID ?
NO
176
PROCESS ERROR
YES
164
AUTHENTICATE MEMBER
166
SUCCESSFUL ?
NO
YES
168
ASSIGN CHANNEL KEYS TO MEMBER
170
SUCCESSFUL ?
NO
YES
172
UPDATE DATABASE
174
DONE

Figure 12

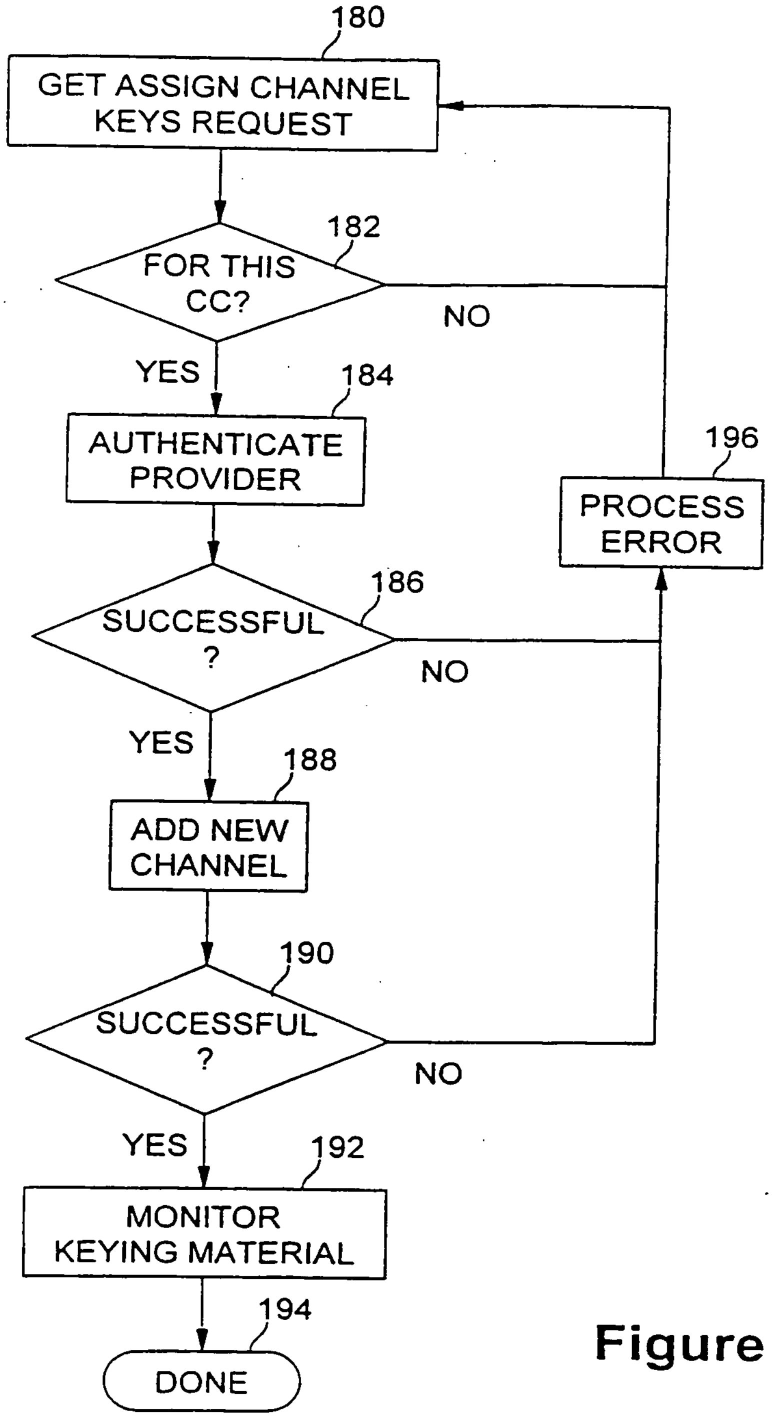

180
GET ASSIGN CHANNEL KEYS REQUEST
182
FOR THIS CC?
NO
YES
184
AUTHENTICATE PROVIDER
196
PROCESS ERROR
186
SUCCESSFUL ?
NO
YES
188
ADD NEW CHANNEL
190
SUCCESSFUL ?
NO
YES
192
MONITOR KEYING MATERIAL
194
DONE

Figure 13

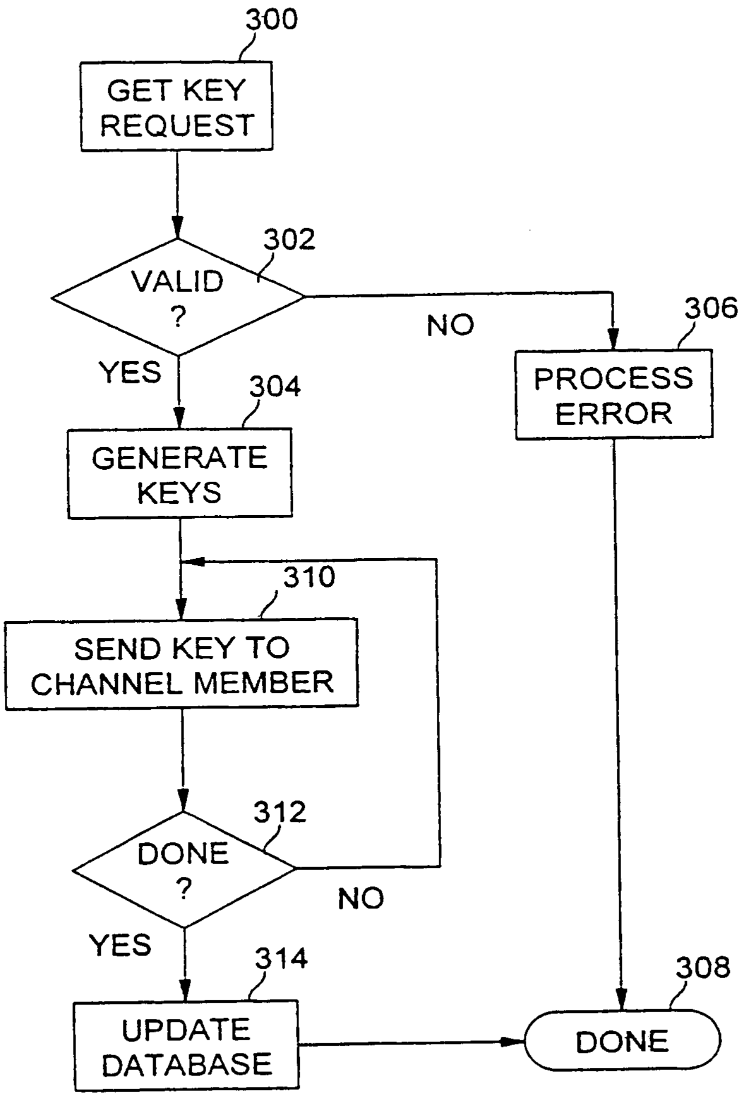

300
GET KEY REQUEST
302
VALID ?
NO
306
PROCESS ERROR
YES
304
GENERATE KEYS
310
SEND KEY TO CHANNEL MEMBER
312
DONE ?
NO
YES
314
UPDATE DATABASE
308
DONE

Figure 14

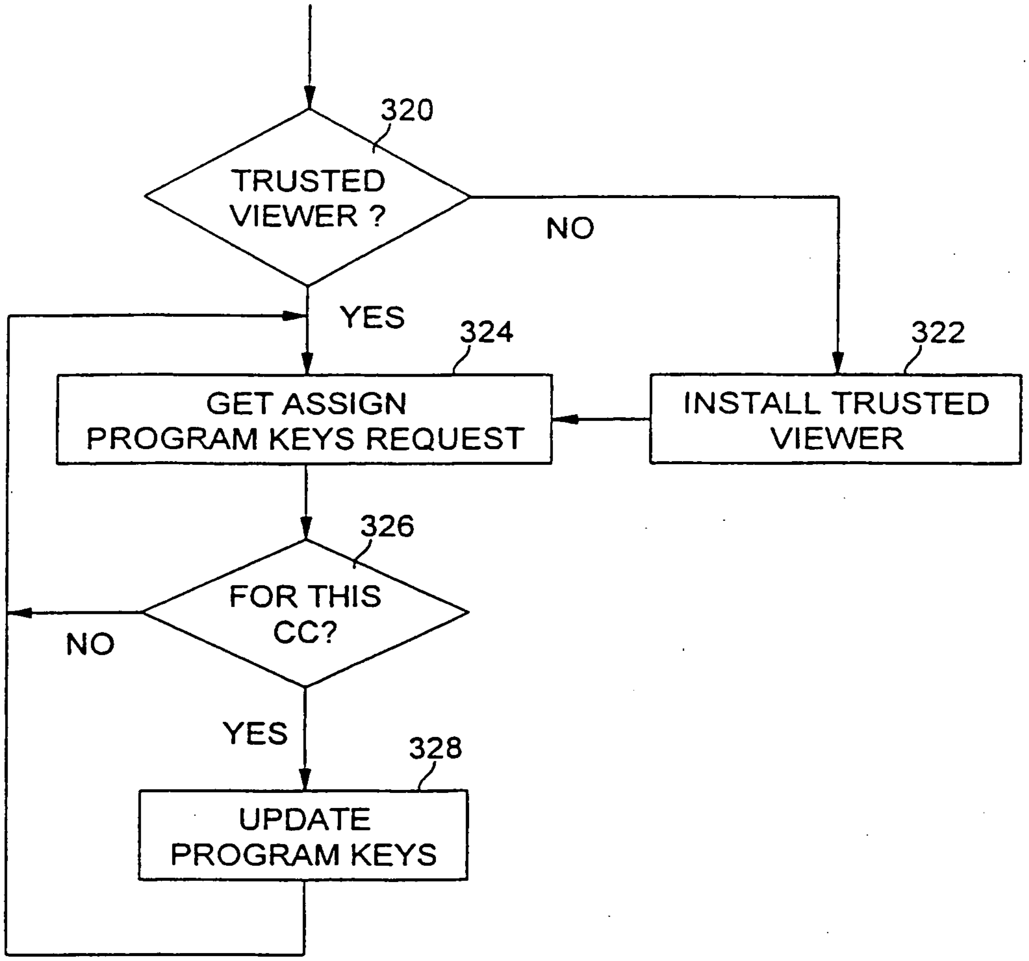

320
TRUSTED VIEWER ?
NO
YES
324
322
GET ASSIGN PROGRAM KEYS REQUEST
INSTALL TRUSTED VIEWER
326
FOR THIS CC?
NO
YES
328
UPDATE PROGRAM KEYS

Figure 15

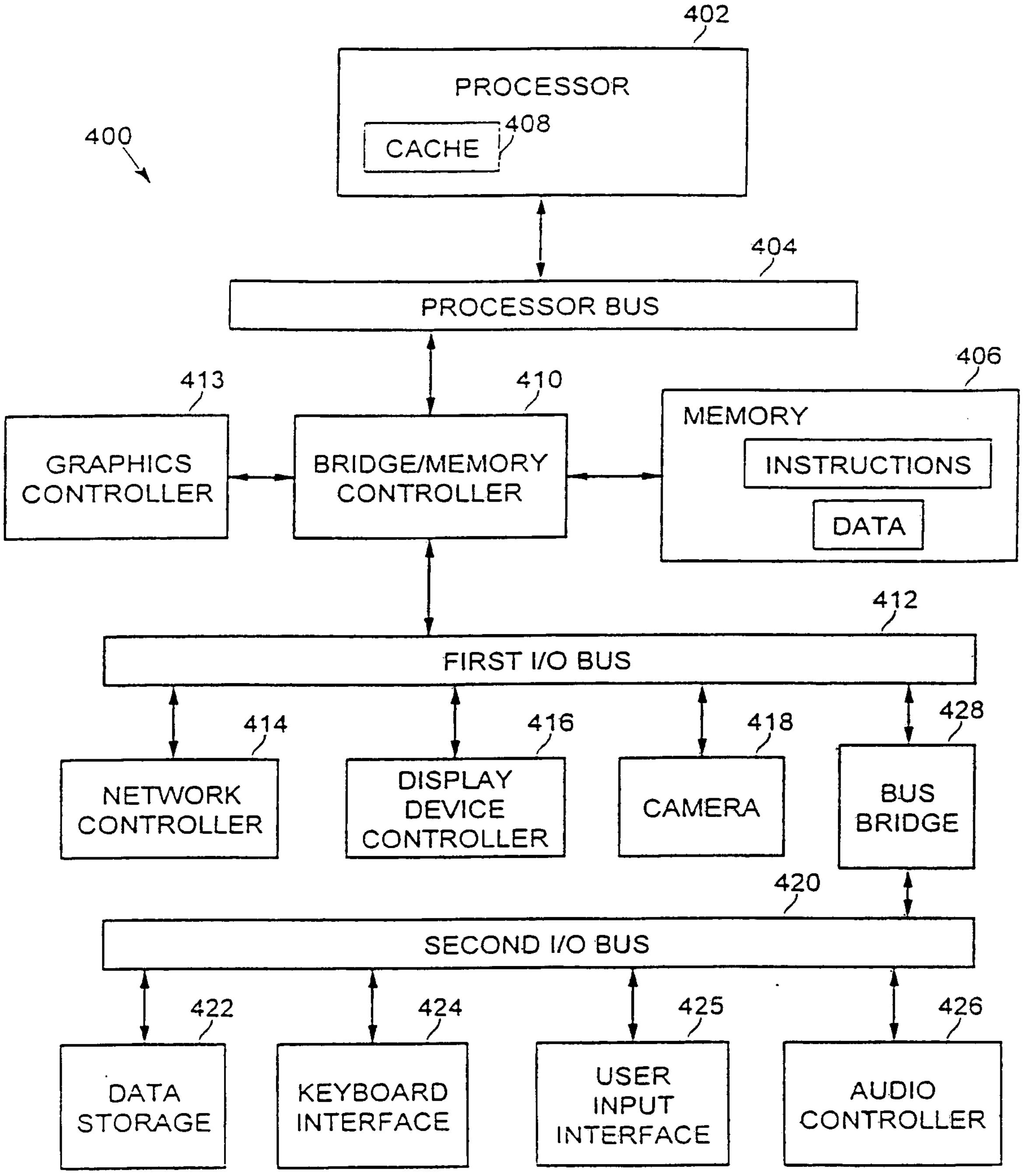

402
PROCESSOR
CACHE
408
400
404
PROCESSOR BUS
413
410
406
GRAPHICS CONTROLLER
BRIDGE/MEMORY CONTROLLER
MEMORY
INSTRUCTIONS
DATA
412
FIRST I/O BUS
414
416
418
428
NETWORK CONTROLLER
DISPLAY DEVICE CONTROLLER
CAMERA
BUS BRIDGE
420
SECOND I/O BUS
422
424
425
426
DATA STORAGE
KEYBOARD INTERFACE
USER INPUT INTERFACE
AUDIO CONTROLLER

Figure 16

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/US 00/21337

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 28649 A (NOKIA OY AB ;SALOMAEKI ARI (FI)) 7 August 1997 (1997-08-07)	1,2, 11-13, 17,25,26
A		21,27
	page 17, line 6 - line 18 figures 1-4 ---	
A	US 5 787 089 A (ALLAN DAVID I ET AL) 28 July 1998 (1998-07-28)	1,2, 11-13, 17,21, 25-27
	column 1, line 9 - line 12 column 4, line 66 -column 5, line 22 figures 1,2 --- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 5 December 2000	Date of mailing of the international search report 14/12/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Tito Martins, J

INTERNATIONAL SEARCH REPORT

Intern. nal Application No
PCT/US 00/21337

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 07149 A (SCIENTIFIC ATLANTA) 11 February 1999 (1999-02-11) page 9, line 25 -page 11, line 22 figures 2A,2B ---	1,2, 11-13, 17,21, 25-27
P,X	US 6 055 314 A (SIMON DANIEL R ET AL) 25 April 2000 (2000-04-25) column 2, line 25 - line 54 column 3, line 36 - line 48 column 4, line 3 - line 7 column 4, line 55 - line 60 column 5, line 3 - line 44 column 6, line 34 - line 40 column 7, line 4 - line 17 column 8, line 60 -column 9, line 3 figures 1-9 -----	1,2,11, 12

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr. nal Application No
PCT/US 00/21337

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9728649 A	07-08-1997	FI 960418 A	31-07-1997
		AU 1548297 A	22-08-1997
		EP 0878096 A	18-11-1998
		JP 2000504169 T	04-04-2000
US 5787089 A	28-07-1998	NONE	
WO 9907149 A	11-02-1999	AU 1581699 A	08-03-1999
		AU 8670598 A	22-02-1999
		AU 8679798 A	22-02-1999
		AU 8679898 A	22-02-1999
		AU 8764298 A	22-02-1999
		AU 8823398 A	22-02-1999
		AU 8823698 A	22-02-1999
		EP 1010323 A	21-06-2000
		EP 1010324 A	21-06-2000
		EP 1010325 A	21-06-2000
		EP 1013091 A	28-06-2000
		EP 1000508 A	17-05-2000
		EP 1000509 A	17-05-2000
		EP 1000511 A	17-05-2000
		WO 9907145 A	11-02-1999
		WO 9907146 A	11-02-1999
		WO 9907147 A	11-02-1999
		WO 9907148 A	11-02-1999
		WO 9909743 A	25-02-1999
		WO 9907150 A	11-02-1999
		US 6105134 A	15-08-2000
US 6055314 A	25-04-2000	NONE	